
Service Authorization Reference

Service Authorization Reference



Service Authorization Reference: Service Authorization Reference

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

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

Table of Contents

Reference	1
Actions, resources, and condition keys	1
Actions table	1
Resource types table	2
Condition keys table	2
AWS Account Management	10
AWS Activate	12
Alexa for Business	13
AmazonMediaImport	22
AWS Amplify	23
AWS Amplify Admin	27
AWS Amplify UI Builder	32
Apache Kafka APIs for Amazon MSK clusters	35
Amazon API Gateway	39
Amazon API Gateway Management	40
Amazon API Gateway Management V2	53
AWS App Mesh	63
AWS App Mesh Preview	68
AWS App Runner	72
AWS AppConfig	78
Amazon AppFlow	84
Amazon AppIntegrations	87
AWS Application Auto Scaling	92
AWS Application Cost Profiler Service	93
Application Discovery Arsenal	95
AWS Application Discovery Service	96
AWS Application Migration Service	102
Amazon AppStream 2.0	112
AWS AppSync	121
AWS Artifact	127
Amazon Athena	128
AWS Audit Manager	132
AWS Auto Scaling	139
AWS Backup	140
AWS Backup Gateway	147
AWS Backup storage	150
AWS Batch	151
AWS Billing and Cost Management	157
AWS Billing Conductor	158
Amazon Braket	162
AWS Budget Service	164
AWS BugBust	166
AWS Certificate Manager	170
AWS Certificate Manager Private Certificate Authority	173
AWS Chatbot	176
Amazon Chime	179
AWS Cloud Control API	203
Amazon Cloud Directory	205
AWS Cloud Map	211
AWS Cloud9	215
AWS CloudFormation	220
Amazon CloudFront	229
AWS CloudHSM	238
Amazon CloudSearch	242

AWS CloudShell	245
AWS CloudTrail	247
Amazon CloudWatch	251
CloudWatch Application Insights	256
Amazon CloudWatch Evidently	258
Amazon CloudWatch Logs	262
AWS CloudWatch RUM	267
Amazon CloudWatch Synthetics	269
AWS CodeArtifact	272
AWS CodeBuild	276
AWS CodeCommit	282
AWS CodeDeploy	292
AWS CodeDeploy secure host commands service	298
Amazon CodeGuru	300
Amazon CodeGuru Profiler	301
Amazon CodeGuru Reviewer	304
AWS CodePipeline	307
AWS CodeStar	312
AWS CodeStar Connections	316
AWS CodeStar Notifications	320
Amazon Cognito Identity	324
Amazon Cognito Sync	327
Amazon Cognito User Pools	330
Amazon Comprehend	338
Amazon Comprehend Medical	352
AWS Compute Optimizer	355
AWS Config	358
Amazon Connect	368
Amazon Connect Customer Profiles	395
Amazon Connect Voice ID	399
Amazon Connect Wisdom	402
AWS Connector Service	406
AWS Control Tower	407
AWS Cost and Usage Report	411
AWS Cost Explorer Service	412
AWS Data Exchange	418
Amazon Data Lifecycle Manager	422
AWS Data Pipeline	424
AWS Database Migration Service	427
Database Query Metadata Service	435
AWS DataSync	437
AWS DeepComposer	442
AWS DeepLens	445
AWS DeepRacer	448
Amazon Detective	456
AWS Device Farm	460
Amazon DevOps Guru	469
AWS Direct Connect	472
AWS Directory Service	480
Amazon DynamoDB	489
Amazon DynamoDB Accelerator (DAX)	497
Amazon EC2	501
Amazon EC2 Auto Scaling	722
Amazon EC2 Image Builder	732
Amazon EC2 Instance Connect	740
AWS Elastic Beanstalk	742
Amazon Elastic Block Store	750

Amazon Elastic Container Registry	752
Amazon Elastic Container Registry Public	757
Amazon Elastic Container Service	760
AWS Elastic Disaster Recovery	769
Amazon Elastic File System	778
Amazon Elastic Inference	783
Amazon Elastic Kubernetes Service	785
Elastic Load Balancing	791
Elastic Load Balancing V2	794
Amazon Elastic MapReduce	801
Amazon Elastic Transcoder	809
Amazon ElastiCache	812
AWS Elemental Appliances and Software	830
AWS Elemental Appliances and Software Activation Service	832
AWS Elemental MediaConnect	834
AWS Elemental MediaConvert	838
AWS Elemental MediaLive	842
AWS Elemental MediaPackage	848
AWS Elemental MediaPackage VOD	851
AWS Elemental MediaStore	854
AWS Elemental MediaTailor	858
Elemental Support Cases	863
Elemental Support Content	865
Amazon EMR on EKS (EMR Containers)	866
Amazon EMR Serverless	869
Amazon EventBridge	871
Amazon EventBridge Schemas	878
AWS Fault Injection Simulator	882
Amazon FinSpace	886
AWS Firewall Manager	889
Amazon Forecast	894
Amazon Fraud Detector	900
Amazon FreeRTOS	914
Amazon FSx	917
Amazon GameLift	924
Amazon GameSparks	934
AWS Global Accelerator	939
AWS Glue	944
AWS Glue DataBrew	960
AWS Ground Station	965
Amazon GroundTruth Labeling	969
Amazon GuardDuty	970
AWS Health APIs and Notifications	976
Amazon HealthLake	979
High-volume outbound communications	982
Amazon Honeycode	985
AWS IAM Access Analyzer	988
Identity And Access Management	992
AWS Identity Store	1009
AWS Identity Synchronization Service	1010
AWS Import Export Disk Service	1012
Amazon Inspector	1013
Amazon Inspector2	1018
Amazon Interactive Video Service	1022
Amazon Interactive Video Service Chat	1027
AWS IoT	1029
AWS IoT 1-Click	1053

AWS IoT Analytics	1056
AWS IoT Core Device Advisor	1060
AWS IoT Core for LoRaWAN	1063
AWS IoT Device Tester	1072
AWS IoT Events	1074
AWS IoT Fleet Hub for Device Management	1078
AWS IoT FleetWise	1080
AWS IoT Greengrass	1085
AWS IoT Greengrass V2	1096
AWS IoT Jobs DataPlane	1101
AWS IoT RoboRunner	1103
AWS IoT SiteWise	1108
AWS IoT Things Graph	1116
AWS IoT TwinMaker	1121
AWS IQ	1125
AWS IQ Permissions	1126
Amazon Kendra	1127
AWS Key Management Service	1134
Amazon Keyspaces (for Apache Cassandra)	1146
Amazon Kinesis	1149
Amazon Kinesis Analytics	1153
Amazon Kinesis Analytics V2	1155
Amazon Kinesis Firehose	1159
Amazon Kinesis Video Streams	1161
AWS Lake Formation	1165
AWS Lambda	1169
Launch Wizard	1176
Amazon Lex	1178
Amazon Lex V2	1184
AWS License Manager	1192
Amazon Lightsail	1196
Amazon Location	1213
Amazon Lookout for Equipment	1219
Amazon Lookout for Metrics	1222
Amazon Lookout for Vision	1226
Amazon Machine Learning	1229
Amazon Macie	1233
Amazon Macie Classic	1239
Amazon Managed Blockchain	1241
Amazon Managed Grafana	1245
Amazon Managed Service for Prometheus	1248
Amazon Managed Streaming for Apache Kafka	1253
Amazon Managed Streaming for Kafka Connect	1257
Amazon Managed Workflows for Apache Airflow	1260
AWS Marketplace	1263
AWS Marketplace Catalog	1266
AWS Marketplace Commerce Analytics Service	1268
AWS Marketplace Entitlement Service	1269
AWS Marketplace Image Building Service	1270
AWS Marketplace Management Portal	1271
AWS Marketplace Metering Service	1273
AWS Marketplace Private Marketplace	1274
AWS Marketplace Procurement Systems Integration	1276
Amazon Mechanical Turk	1278
Amazon MemoryDB	1282
Amazon Message Delivery Service	1290
AWS Microservice Extractor for .NET	1291

AWS Migration Hub	1292
AWS Migration Hub Orchestrator	1295
AWS Migration Hub Refactor Spaces	1298
AWS Migration Hub Strategy Recommendations	1305
Amazon Mobile Analytics	1308
AWS Mobile Hub	1309
Amazon Monitron	1312
Amazon MQ	1315
Amazon Neptune	1318
AWS Network Firewall	1319
Network Manager	1324
Amazon Nimble Studio	1333
Amazon OpenSearch Service (successor to Amazon Elasticsearch Service)	1341
AWS OpsWorks	1351
AWS OpsWorks Configuration Management	1357
AWS Organizations	1360
AWS Outposts	1367
AWS Panorama	1369
AWS Performance Insights	1377
Amazon Personalize	1378
Amazon Pinpoint	1384
Amazon Pinpoint Email Service	1396
Amazon Pinpoint SMS and Voice Service	1404
Amazon Pinpoint SMS Voice V2	1405
Amazon Polly	1411
AWS Price List	1413
AWS Proton	1414
AWS Purchase Orders Console	1426
Amazon QLDB	1427
Amazon QuickSight	1431
Amazon RDS	1446
Amazon RDS Data API	1469
Amazon RDS IAM Authentication	1472
Recycle Bin	1473
Amazon Redshift	1475
Amazon Redshift Data API	1490
Amazon Rekognition	1492
AWS Resilience Hub Service	1498
AWS Resource Access Manager	1504
Amazon Resource Group Tagging API	1509
AWS Resource Groups	1511
Amazon RHEL Knowledgebase Portal	1514
AWS RoboMaker	1515
Amazon Route 53	1522
Amazon Route 53 Domains	1529
Amazon Route 53 Recovery Cluster	1533
Amazon Route 53 Recovery Controls	1534
Amazon Route 53 Recovery Readiness	1538
Amazon Route 53 Resolver	1542
Amazon S3	1551
Amazon S3 Glacier	1613
Amazon S3 Object Lambda	1617
Amazon S3 on Outposts	1624
Amazon SageMaker	1642
AWS Savings Plans	1685
AWS Secrets Manager	1687
AWS Security Hub	1696

AWS Security Token Service	1703
AWS Server Migration Service	1711
AWS Serverless Application Repository	1714
AWS Service Catalog	1717
Service Quotas	1727
Amazon SES	1730
Amazon Session Manager Message Gateway Service	1738
AWS Shield	1740
AWS Signer	1745
Amazon Simple Email Service v2	1748
Amazon Simple Workflow Service	1760
Amazon SimpleDB	1768
AWS Snow Device Management	1770
AWS Snowball	1772
Amazon SNS	1775
AWS SQL Workbench	1780
Amazon SQS	1786
AWS SSO	1788
AWS SSO Directory	1796
AWS Step Functions	1801
Amazon Storage Gateway	1804
Amazon Sumerian	1814
AWS Support	1816
AWS Sustainability	1818
AWS Systems Manager	1819
AWS Systems Manager GUI Connect	1836
AWS Systems Manager Incident Manager	1837
AWS Systems Manager Incident Manager Contacts	1841
AWS Tag Editor	1844
AWS Tax Settings	1845
Amazon Textract	1846
Amazon Timestream	1848
AWS Tiros	1851
Amazon Transcribe	1853
AWS Transfer Family	1859
Amazon Translate	1863
AWS Trusted Advisor	1865
AWS WAF	1868
AWS WAF Regional	1875
AWS WAF V2	1883
AWS Well-Architected Tool	1890
Amazon WorkDocs	1894
Amazon WorkLink	1899
Amazon WorkMail	1903
Amazon WorkMail Message Flow	1914
Amazon WorkSpaces	1916
Amazon WorkSpaces Application Manager	1922
Amazon WorkSpaces Web	1923
AWS X-Ray	1928
Related resources	1932

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 \(p. 1\)](#)
- [Related resources \(p. 1932\)](#)

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. In addition, a service might define some actions that don't directly correspond to an API operation. 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 includes any additional permissions that you must have, in addition to the permission for the action itself, to successfully call the action. This can be required if the action accesses more than one resource.

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 IAM user's name or a [policy variable](#) that contains an IAM user's name. For more information about ARNs, see [IAM ARNs](#).
- The **Condition keys** column specifies condition context keys that you can include in an IAM policy statement only when both this resource and a supporting action from the table above are included in the statement.

The condition keys table

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

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

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

Topics

- [Actions, resources, and condition keys for AWS Account Management \(p. 10\)](#)
- [Actions, resources, and condition keys for AWS Activate \(p. 12\)](#)
- [Actions, resources, and condition keys for Alexa for Business \(p. 13\)](#)
- [Actions, resources, and condition keys for AmazonMediaImport \(p. 22\)](#)
- [Actions, resources, and condition keys for AWS Amplify \(p. 23\)](#)
- [Actions, resources, and condition keys for AWS Amplify Admin \(p. 27\)](#)
- [Actions, resources, and condition keys for AWS Amplify UI Builder \(p. 32\)](#)
- [Actions, resources, and condition keys for Apache Kafka APIs for Amazon MSK clusters \(p. 35\)](#)
- [Actions, resources, and condition keys for Amazon API Gateway \(p. 39\)](#)
- [Actions, resources, and condition keys for Amazon API Gateway Management \(p. 40\)](#)
- [Actions, resources, and condition keys for Amazon API Gateway Management V2 \(p. 53\)](#)

- Actions, resources, and condition keys for AWS App Mesh (p. 63)
- Actions, resources, and condition keys for AWS App Mesh Preview (p. 68)
- Actions, resources, and condition keys for AWS App Runner (p. 72)
- Actions, resources, and condition keys for AWS AppConfig (p. 78)
- Actions, resources, and condition keys for Amazon AppFlow (p. 84)
- Actions, resources, and condition keys for Amazon AppIntegrations (p. 87)
- Actions, resources, and condition keys for AWS Application Auto Scaling (p. 92)
- Actions, resources, and condition keys for AWS Application Cost Profiler Service (p. 93)
- Actions, resources, and condition keys for Application Discovery Arsenal (p. 95)
- Actions, resources, and condition keys for AWS Application Discovery Service (p. 96)
- Actions, resources, and condition keys for AWS Application Migration Service (p. 102)
- Actions, resources, and condition keys for Amazon AppStream 2.0 (p. 112)
- Actions, resources, and condition keys for AWS AppSync (p. 121)
- Actions, resources, and condition keys for AWS Artifact (p. 127)
- Actions, resources, and condition keys for Amazon Athena (p. 128)
- Actions, resources, and condition keys for AWS Audit Manager (p. 132)
- Actions, resources, and condition keys for AWS Auto Scaling (p. 139)
- Actions, resources, and condition keys for AWS Backup (p. 140)
- Actions, resources, and condition keys for AWS Backup Gateway (p. 147)
- Actions, resources, and condition keys for AWS Backup storage (p. 150)
- Actions, resources, and condition keys for AWS Batch (p. 151)
- Actions, resources, and condition keys for AWS Billing and Cost Management (p. 157)
- Actions, resources, and condition keys for AWS Billing Conductor (p. 158)
- Actions, resources, and condition keys for Amazon Braket (p. 162)
- Actions, resources, and condition keys for AWS Budget Service (p. 164)
- Actions, resources, and condition keys for AWS BugBust (p. 166)
- Actions, resources, and condition keys for AWS Certificate Manager (p. 170)
- Actions, resources, and condition keys for AWS Certificate Manager Private Certificate Authority (p. 173)
- Actions, resources, and condition keys for AWS Chatbot (p. 176)
- Actions, resources, and condition keys for Amazon Chime (p. 179)
- Actions, resources, and condition keys for AWS Cloud Control API (p. 203)
- Actions, resources, and condition keys for Amazon Cloud Directory (p. 205)
- Actions, resources, and condition keys for AWS Cloud Map (p. 211)
- Actions, resources, and condition keys for AWS Cloud9 (p. 215)
- Actions, resources, and condition keys for AWS CloudFormation (p. 220)
- Actions, resources, and condition keys for Amazon CloudFront (p. 229)
- Actions, resources, and condition keys for AWS CloudHSM (p. 238)
- Actions, resources, and condition keys for Amazon CloudSearch (p. 242)
- Actions, resources, and condition keys for AWS CloudShell (p. 245)
- Actions, resources, and condition keys for AWS CloudTrail (p. 247)
- Actions, resources, and condition keys for Amazon CloudWatch (p. 251)
- Actions, resources, and condition keys for CloudWatch Application Insights (p. 256)
- Actions, resources, and condition keys for Amazon CloudWatch Evidently (p. 258)

- [Actions, resources, and condition keys for Amazon CloudWatch Logs \(p. 262\)](#)
- [Actions, resources, and condition keys for AWS CloudWatch RUM \(p. 267\)](#)
- [Actions, resources, and condition keys for Amazon CloudWatch Synthetics \(p. 269\)](#)
- [Actions, resources, and condition keys for AWS CodeArtifact \(p. 272\)](#)
- [Actions, resources, and condition keys for AWS CodeBuild \(p. 276\)](#)
- [Actions, resources, and condition keys for AWS CodeCommit \(p. 282\)](#)
- [Actions, resources, and condition keys for AWS CodeDeploy \(p. 292\)](#)
- [Actions, resources, and condition keys for AWS CodeDeploy secure host commands service \(p. 298\)](#)
- [Actions, resources, and condition keys for Amazon CodeGuru \(p. 300\)](#)
- [Actions, resources, and condition keys for Amazon CodeGuru Profiler \(p. 301\)](#)
- [Actions, resources, and condition keys for Amazon CodeGuru Reviewer \(p. 304\)](#)
- [Actions, resources, and condition keys for AWS CodePipeline \(p. 307\)](#)
- [Actions, resources, and condition keys for AWS CodeStar \(p. 312\)](#)
- [Actions, resources, and condition keys for AWS CodeStar Connections \(p. 316\)](#)
- [Actions, resources, and condition keys for AWS CodeStar Notifications \(p. 320\)](#)
- [Actions, resources, and condition keys for Amazon Cognito Identity \(p. 324\)](#)
- [Actions, resources, and condition keys for Amazon Cognito Sync \(p. 327\)](#)
- [Actions, resources, and condition keys for Amazon Cognito User Pools \(p. 330\)](#)
- [Actions, resources, and condition keys for Amazon Comprehend \(p. 338\)](#)
- [Actions, resources, and condition keys for Amazon Comprehend Medical \(p. 352\)](#)
- [Actions, resources, and condition keys for AWS Compute Optimizer \(p. 355\)](#)
- [Actions, resources, and condition keys for AWS Config \(p. 358\)](#)
- [Actions, resources, and condition keys for Amazon Connect \(p. 368\)](#)
- [Actions, resources, and condition keys for Amazon Connect Customer Profiles \(p. 395\)](#)
- [Actions, resources, and condition keys for Amazon Connect Voice ID \(p. 399\)](#)
- [Actions, resources, and condition keys for Amazon Connect Wisdom \(p. 402\)](#)
- [Actions, resources, and condition keys for AWS Connector Service \(p. 406\)](#)
- [Actions, resources, and condition keys for AWS Control Tower \(p. 407\)](#)
- [Actions, resources, and condition keys for AWS Cost and Usage Report \(p. 411\)](#)
- [Actions, resources, and condition keys for AWS Cost Explorer Service \(p. 412\)](#)
- [Actions, resources, and condition keys for AWS Data Exchange \(p. 418\)](#)
- [Actions, resources, and condition keys for Amazon Data Lifecycle Manager \(p. 422\)](#)
- [Actions, resources, and condition keys for AWS Data Pipeline \(p. 424\)](#)
- [Actions, resources, and condition keys for AWS Database Migration Service \(p. 427\)](#)
- [Actions, resources, and condition keys for Database Query Metadata Service \(p. 435\)](#)
- [Actions, resources, and condition keys for AWS DataSync \(p. 437\)](#)
- [Actions, resources, and condition keys for AWS DeepComposer \(p. 442\)](#)
- [Actions, resources, and condition keys for AWS DeepLens \(p. 445\)](#)
- [Actions, resources, and condition keys for AWS DeepRacer \(p. 448\)](#)
- [Actions, resources, and condition keys for Amazon Detective \(p. 456\)](#)
- [Actions, resources, and condition keys for AWS Device Farm \(p. 460\)](#)
- [Actions, resources, and condition keys for Amazon DevOps Guru \(p. 469\)](#)
- [Actions, resources, and condition keys for AWS Direct Connect \(p. 472\)](#)

- [Actions, resources, and condition keys for AWS Directory Service \(p. 480\)](#)
- [Actions, resources, and condition keys for Amazon DynamoDB \(p. 489\)](#)
- [Actions, resources, and condition keys for Amazon DynamoDB Accelerator \(DAX\) \(p. 497\)](#)
- [Actions, resources, and condition keys for Amazon EC2 \(p. 501\)](#)
- [Actions, resources, and condition keys for Amazon EC2 Auto Scaling \(p. 722\)](#)
- [Actions, resources, and condition keys for Amazon EC2 Image Builder \(p. 732\)](#)
- [Actions, resources, and condition keys for Amazon EC2 Instance Connect \(p. 740\)](#)
- [Actions, resources, and condition keys for AWS Elastic Beanstalk \(p. 742\)](#)
- [Actions, resources, and condition keys for Amazon Elastic Block Store \(p. 750\)](#)
- [Actions, resources, and condition keys for Amazon Elastic Container Registry \(p. 752\)](#)
- [Actions, resources, and condition keys for Amazon Elastic Container Registry Public \(p. 757\)](#)
- [Actions, resources, and condition keys for Amazon Elastic Container Service \(p. 760\)](#)
- [Actions, resources, and condition keys for AWS Elastic Disaster Recovery \(p. 769\)](#)
- [Actions, resources, and condition keys for Amazon Elastic File System \(p. 778\)](#)
- [Actions, resources, and condition keys for Amazon Elastic Inference \(p. 783\)](#)
- [Actions, resources, and condition keys for Amazon Elastic Kubernetes Service \(p. 785\)](#)
- [Actions, resources, and condition keys for Elastic Load Balancing \(p. 791\)](#)
- [Actions, resources, and condition keys for Elastic Load Balancing V2 \(p. 794\)](#)
- [Actions, resources, and condition keys for Amazon Elastic MapReduce \(p. 801\)](#)
- [Actions, resources, and condition keys for Amazon Elastic Transcoder \(p. 809\)](#)
- [Actions, resources, and condition keys for Amazon ElastiCache \(p. 812\)](#)
- [Actions, resources, and condition keys for AWS Elemental Appliances and Software \(p. 830\)](#)
- [Actions, resources, and condition keys for AWS Elemental Appliances and Software Activation Service \(p. 832\)](#)
- [Actions, resources, and condition keys for AWS Elemental MediaConnect \(p. 834\)](#)
- [Actions, resources, and condition keys for AWS Elemental MediaConvert \(p. 838\)](#)
- [Actions, resources, and condition keys for AWS Elemental MediaLive \(p. 842\)](#)
- [Actions, resources, and condition keys for AWS Elemental MediaPackage \(p. 848\)](#)
- [Actions, resources, and condition keys for AWS Elemental MediaPackage VOD \(p. 851\)](#)
- [Actions, resources, and condition keys for AWS Elemental MediaStore \(p. 854\)](#)
- [Actions, resources, and condition keys for AWS Elemental MediaTailor \(p. 858\)](#)
- [Actions, resources, and condition keys for Elemental Support Cases \(p. 863\)](#)
- [Actions, resources, and condition keys for Elemental Support Content \(p. 865\)](#)
- [Actions, resources, and condition keys for Amazon EMR on EKS \(EMR Containers\) \(p. 866\)](#)
- [Actions, resources, and condition keys for Amazon EMR Serverless \(p. 869\)](#)
- [Actions, resources, and condition keys for Amazon EventBridge \(p. 871\)](#)
- [Actions, resources, and condition keys for Amazon EventBridge Schemas \(p. 878\)](#)
- [Actions, resources, and condition keys for AWS Fault Injection Simulator \(p. 882\)](#)
- [Actions, resources, and condition keys for Amazon FinSpace \(p. 886\)](#)
- [Actions, resources, and condition keys for AWS Firewall Manager \(p. 889\)](#)
- [Actions, resources, and condition keys for Amazon Forecast \(p. 894\)](#)
- [Actions, resources, and condition keys for Amazon Fraud Detector \(p. 900\)](#)
- [Actions, resources, and condition keys for Amazon FreeRTOS \(p. 914\)](#)
- [Actions, resources, and condition keys for Amazon FSx \(p. 917\)](#)

- [Actions, resources, and condition keys for Amazon GameLift \(p. 924\)](#)
- [Actions, resources, and condition keys for Amazon GameSparks \(p. 934\)](#)
- [Actions, resources, and condition keys for AWS Global Accelerator \(p. 939\)](#)
- [Actions, resources, and condition keys for AWS Glue \(p. 944\)](#)
- [Actions, resources, and condition keys for AWS Glue DataBrew \(p. 960\)](#)
- [Actions, resources, and condition keys for AWS Ground Station \(p. 965\)](#)
- [Actions, resources, and condition keys for Amazon GroundTruth Labeling \(p. 969\)](#)
- [Actions, resources, and condition keys for Amazon GuardDuty \(p. 970\)](#)
- [Actions, resources, and condition keys for AWS Health APIs and Notifications \(p. 976\)](#)
- [Actions, resources, and condition keys for Amazon HealthLake \(p. 979\)](#)
- [Actions, resources, and condition keys for High-volume outbound communications \(p. 982\)](#)
- [Actions, resources, and condition keys for Amazon Honeycode \(p. 985\)](#)
- [Actions, resources, and condition keys for AWS IAM Access Analyzer \(p. 988\)](#)
- [Actions, resources, and condition keys for Identity And Access Management \(p. 992\)](#)
- [Actions, resources, and condition keys for AWS Identity Store \(p. 1009\)](#)
- [Actions, resources, and condition keys for AWS Identity Synchronization Service \(p. 1010\)](#)
- [Actions, resources, and condition keys for AWS Import Export Disk Service \(p. 1012\)](#)
- [Actions, resources, and condition keys for Amazon Inspector \(p. 1013\)](#)
- [Actions, resources, and condition keys for Amazon Inspector2 \(p. 1018\)](#)
- [Actions, resources, and condition keys for Amazon Interactive Video Service \(p. 1022\)](#)
- [Actions, resources, and condition keys for Amazon Interactive Video Service Chat \(p. 1027\)](#)
- [Actions, resources, and condition keys for AWS IoT \(p. 1029\)](#)
- [Actions, resources, and condition keys for AWS IoT 1-Click \(p. 1053\)](#)
- [Actions, resources, and condition keys for AWS IoT Analytics \(p. 1056\)](#)
- [Actions, resources, and condition keys for AWS IoT Core Device Advisor \(p. 1060\)](#)
- [Actions, resources, and condition keys for AWS IoT Core for LoRaWAN \(p. 1063\)](#)
- [Actions, resources, and condition keys for AWS IoT Device Tester \(p. 1072\)](#)
- [Actions, resources, and condition keys for AWS IoT Events \(p. 1074\)](#)
- [Actions, resources, and condition keys for AWS IoT Fleet Hub for Device Management \(p. 1078\)](#)
- [Actions, resources, and condition keys for AWS IoT FleetWise \(p. 1080\)](#)
- [Actions, resources, and condition keys for AWS IoT Greengrass \(p. 1085\)](#)
- [Actions, resources, and condition keys for AWS IoT Greengrass V2 \(p. 1096\)](#)
- [Actions, resources, and condition keys for AWS IoT Jobs DataPlane \(p. 1101\)](#)
- [Actions, resources, and condition keys for AWS IoT RoboRunner \(p. 1103\)](#)
- [Actions, resources, and condition keys for AWS IoT SiteWise \(p. 1108\)](#)
- [Actions, resources, and condition keys for AWS IoT Things Graph \(p. 1116\)](#)
- [Actions, resources, and condition keys for AWS IoT TwinMaker \(p. 1121\)](#)
- [Actions, resources, and condition keys for AWS IQ \(p. 1125\)](#)
- [Actions, resources, and condition keys for AWS IQ Permissions \(p. 1126\)](#)
- [Actions, resources, and condition keys for Amazon Kendra \(p. 1127\)](#)
- [Actions, resources, and condition keys for AWS Key Management Service \(p. 1134\)](#)
- [Actions, resources, and condition keys for Amazon Keyspaces \(for Apache Cassandra\) \(p. 1146\)](#)
- [Actions, resources, and condition keys for Amazon Kinesis \(p. 1149\)](#)

- [Actions, resources, and condition keys for Amazon Kinesis Analytics \(p. 1153\)](#)
- [Actions, resources, and condition keys for Amazon Kinesis Analytics V2 \(p. 1155\)](#)
- [Actions, resources, and condition keys for Amazon Kinesis Firehose \(p. 1159\)](#)
- [Actions, resources, and condition keys for Amazon Kinesis Video Streams \(p. 1161\)](#)
- [Actions, resources, and condition keys for AWS Lake Formation \(p. 1165\)](#)
- [Actions, resources, and condition keys for AWS Lambda \(p. 1169\)](#)
- [Actions, resources, and condition keys for Launch Wizard \(p. 1176\)](#)
- [Actions, resources, and condition keys for Amazon Lex \(p. 1178\)](#)
- [Actions, resources, and condition keys for Amazon Lex V2 \(p. 1184\)](#)
- [Actions, resources, and condition keys for AWS License Manager \(p. 1192\)](#)
- [Actions, resources, and condition keys for Amazon Lightsail \(p. 1196\)](#)
- [Actions, resources, and condition keys for Amazon Location \(p. 1213\)](#)
- [Actions, resources, and condition keys for Amazon Lookout for Equipment \(p. 1219\)](#)
- [Actions, resources, and condition keys for Amazon Lookout for Metrics \(p. 1222\)](#)
- [Actions, resources, and condition keys for Amazon Lookout for Vision \(p. 1226\)](#)
- [Actions, resources, and condition keys for Amazon Machine Learning \(p. 1229\)](#)
- [Actions, resources, and condition keys for Amazon Macie \(p. 1233\)](#)
- [Actions, resources, and condition keys for Amazon Macie Classic \(p. 1239\)](#)
- [Actions, resources, and condition keys for Amazon Managed Blockchain \(p. 1241\)](#)
- [Actions, resources, and condition keys for Amazon Managed Grafana \(p. 1245\)](#)
- [Actions, resources, and condition keys for Amazon Managed Service for Prometheus \(p. 1248\)](#)
- [Actions, resources, and condition keys for Amazon Managed Streaming for Apache Kafka \(p. 1253\)](#)
- [Actions, resources, and condition keys for Amazon Managed Streaming for Kafka Connect \(p. 1257\)](#)
- [Actions, resources, and condition keys for Amazon Managed Workflows for Apache Airflow \(p. 1260\)](#)
- [Actions, resources, and condition keys for AWS Marketplace \(p. 1263\)](#)
- [Actions, resources, and condition keys for AWS Marketplace Catalog \(p. 1266\)](#)
- [Actions, resources, and condition keys for AWS Marketplace Commerce Analytics Service \(p. 1268\)](#)
- [Actions, resources, and condition keys for AWS Marketplace Entitlement Service \(p. 1269\)](#)
- [Actions, resources, and condition keys for AWS Marketplace Image Building Service \(p. 1270\)](#)
- [Actions, resources, and condition keys for AWS Marketplace Management Portal \(p. 1271\)](#)
- [Actions, resources, and condition keys for AWS Marketplace Metering Service \(p. 1273\)](#)
- [Actions, resources, and condition keys for AWS Marketplace Private Marketplace \(p. 1274\)](#)
- [Actions, resources, and condition keys for AWS Marketplace Procurement Systems Integration \(p. 1276\)](#)
- [Actions, resources, and condition keys for Amazon Mechanical Turk \(p. 1278\)](#)
- [Actions, resources, and condition keys for Amazon MemoryDB \(p. 1282\)](#)
- [Actions, resources, and condition keys for Amazon Message Delivery Service \(p. 1290\)](#)
- [Actions, resources, and condition keys for AWS Microservice Extractor for .NET \(p. 1291\)](#)
- [Actions, resources, and condition keys for AWS Migration Hub \(p. 1292\)](#)
- [Actions, resources, and condition keys for AWS Migration Hub Orchestrator \(p. 1295\)](#)
- [Actions, resources, and condition keys for AWS Migration Hub Refactor Spaces \(p. 1298\)](#)
- [Actions, resources, and condition keys for AWS Migration Hub Strategy Recommendations \(p. 1305\)](#)
- [Actions, resources, and condition keys for Amazon Mobile Analytics \(p. 1308\)](#)
- [Actions, resources, and condition keys for AWS Mobile Hub \(p. 1309\)](#)

- [Actions, resources, and condition keys for Amazon Monitron \(p. 1312\)](#)
- [Actions, resources, and condition keys for Amazon MQ \(p. 1315\)](#)
- [Actions, resources, and condition keys for Amazon Neptune \(p. 1318\)](#)
- [Actions, resources, and condition keys for AWS Network Firewall \(p. 1319\)](#)
- [Actions, resources, and condition keys for Network Manager \(p. 1324\)](#)
- [Actions, resources, and condition keys for Amazon Nimble Studio \(p. 1333\)](#)
- [Actions, resources, and condition keys for Amazon OpenSearch Service \(successor to Amazon Elasticsearch Service\) \(p. 1341\)](#)
- [Actions, resources, and condition keys for AWS OpsWorks \(p. 1351\)](#)
- [Actions, resources, and condition keys for AWS OpsWorks Configuration Management \(p. 1357\)](#)
- [Actions, resources, and condition keys for AWS Organizations \(p. 1360\)](#)
- [Actions, resources, and condition keys for AWS Outposts \(p. 1367\)](#)
- [Actions, resources, and condition keys for AWS Panorama \(p. 1369\)](#)
- [Actions, resources, and condition keys for AWS Performance Insights \(p. 1377\)](#)
- [Actions, resources, and condition keys for Amazon Personalize \(p. 1378\)](#)
- [Actions, resources, and condition keys for Amazon Pinpoint \(p. 1384\)](#)
- [Actions, resources, and condition keys for Amazon Pinpoint Email Service \(p. 1396\)](#)
- [Actions, resources, and condition keys for Amazon Pinpoint SMS and Voice Service \(p. 1404\)](#)
- [Actions, resources, and condition keys for Amazon Pinpoint SMS Voice V2 \(p. 1405\)](#)
- [Actions, resources, and condition keys for Amazon Polly \(p. 1411\)](#)
- [Actions, resources, and condition keys for AWS Price List \(p. 1413\)](#)
- [Actions, resources, and condition keys for AWS Proton \(p. 1414\)](#)
- [Actions, resources, and condition keys for AWS Purchase Orders Console \(p. 1426\)](#)
- [Actions, resources, and condition keys for Amazon QLDB \(p. 1427\)](#)
- [Actions, resources, and condition keys for Amazon QuickSight \(p. 1431\)](#)
- [Actions, resources, and condition keys for Amazon RDS \(p. 1446\)](#)
- [Actions, resources, and condition keys for Amazon RDS Data API \(p. 1469\)](#)
- [Actions, resources, and condition keys for Amazon RDS IAM Authentication \(p. 1472\)](#)
- [Actions, resources, and condition keys for Recycle Bin \(p. 1473\)](#)
- [Actions, resources, and condition keys for Amazon Redshift \(p. 1475\)](#)
- [Actions, resources, and condition keys for Amazon Redshift Data API \(p. 1490\)](#)
- [Actions, resources, and condition keys for Amazon Rekognition \(p. 1492\)](#)
- [Actions, resources, and condition keys for AWS Resilience Hub Service \(p. 1498\)](#)
- [Actions, resources, and condition keys for AWS Resource Access Manager \(p. 1504\)](#)
- [Actions, resources, and condition keys for Amazon Resource Group Tagging API \(p. 1509\)](#)
- [Actions, resources, and condition keys for AWS Resource Groups \(p. 1511\)](#)
- [Actions, resources, and condition keys for Amazon RHEL Knowledgebase Portal \(p. 1514\)](#)
- [Actions, resources, and condition keys for AWS RoboMaker \(p. 1515\)](#)
- [Actions, resources, and condition keys for Amazon Route 53 \(p. 1522\)](#)
- [Actions, resources, and condition keys for Amazon Route 53 Domains \(p. 1529\)](#)
- [Actions, resources, and condition keys for Amazon Route 53 Recovery Cluster \(p. 1533\)](#)
- [Actions, resources, and condition keys for Amazon Route 53 Recovery Controls \(p. 1534\)](#)
- [Actions, resources, and condition keys for Amazon Route 53 Recovery Readiness \(p. 1538\)](#)
- [Actions, resources, and condition keys for Amazon Route 53 Resolver \(p. 1542\)](#)

- Actions, resources, and condition keys for Amazon S3 (p. 1551)
- Actions, resources, and condition keys for Amazon S3 Glacier (p. 1613)
- Actions, resources, and condition keys for Amazon S3 Object Lambda (p. 1617)
- Actions, resources, and condition keys for Amazon S3 on Outposts (p. 1624)
- Actions, resources, and condition keys for Amazon SageMaker (p. 1642)
- Actions, resources, and condition keys for AWS Savings Plans (p. 1685)
- Actions, resources, and condition keys for AWS Secrets Manager (p. 1687)
- Actions, resources, and condition keys for AWS Security Hub (p. 1696)
- Actions, resources, and condition keys for AWS Security Token Service (p. 1703)
- Actions, resources, and condition keys for AWS Server Migration Service (p. 1711)
- Actions, resources, and condition keys for AWS Serverless Application Repository (p. 1714)
- Actions, resources, and condition keys for AWS Service Catalog (p. 1717)
- Actions, resources, and condition keys for Service Quotas (p. 1727)
- Actions, resources, and condition keys for Amazon SES (p. 1730)
- Actions, resources, and condition keys for Amazon Session Manager Message Gateway Service (p. 1738)
- Actions, resources, and condition keys for AWS Shield (p. 1740)
- Actions, resources, and condition keys for AWS Signer (p. 1745)
- Actions, resources, and condition keys for Amazon Simple Email Service v2 (p. 1748)
- Actions, resources, and condition keys for Amazon Simple Workflow Service (p. 1760)
- Actions, resources, and condition keys for Amazon SimpleDB (p. 1768)
- Actions, resources, and condition keys for AWS Snow Device Management (p. 1770)
- Actions, resources, and condition keys for AWS Snowball (p. 1772)
- Actions, resources, and condition keys for Amazon SNS (p. 1775)
- Actions, resources, and condition keys for AWS SQL Workbench (p. 1780)
- Actions, resources, and condition keys for Amazon SQS (p. 1786)
- Actions, resources, and condition keys for AWS SSO (p. 1788)
- Actions, resources, and condition keys for AWS SSO Directory (p. 1796)
- Actions, resources, and condition keys for AWS Step Functions (p. 1801)
- Actions, resources, and condition keys for Amazon Storage Gateway (p. 1804)
- Actions, resources, and condition keys for Amazon Sumerian (p. 1814)
- Actions, resources, and condition keys for AWS Support (p. 1816)
- Actions, resources, and condition keys for AWS Sustainability (p. 1818)
- Actions, resources, and condition keys for AWS Systems Manager (p. 1819)
- Actions, resources, and condition keys for AWS Systems Manager GUI Connect (p. 1836)
- Actions, resources, and condition keys for AWS Systems Manager Incident Manager (p. 1837)
- Actions, resources, and condition keys for AWS Systems Manager Incident Manager Contacts (p. 1841)
- Actions, resources, and condition keys for AWS Tag Editor (p. 1844)
- Actions, resources, and condition keys for AWS Tax Settings (p. 1845)
- Actions, resources, and condition keys for Amazon Textract (p. 1846)
- Actions, resources, and condition keys for Amazon Timestream (p. 1848)
- Actions, resources, and condition keys for AWS Tiros (p. 1851)
- Actions, resources, and condition keys for Amazon Transcribe (p. 1853)

- [Actions, resources, and condition keys for AWS Transfer Family \(p. 1859\)](#)
- [Actions, resources, and condition keys for Amazon Translate \(p. 1863\)](#)
- [Actions, resources, and condition keys for AWS Trusted Advisor \(p. 1865\)](#)
- [Actions, resources, and condition keys for AWS WAF \(p. 1868\)](#)
- [Actions, resources, and condition keys for AWS WAF Regional \(p. 1875\)](#)
- [Actions, resources, and condition keys for AWS WAF V2 \(p. 1883\)](#)
- [Actions, resources, and condition keys for AWS Well-Architected Tool \(p. 1890\)](#)
- [Actions, resources, and condition keys for Amazon WorkDocs \(p. 1894\)](#)
- [Actions, resources, and condition keys for Amazon WorkLink \(p. 1899\)](#)
- [Actions, resources, and condition keys for Amazon WorkMail \(p. 1903\)](#)
- [Actions, resources, and condition keys for Amazon WorkMail Message Flow \(p. 1914\)](#)
- [Actions, resources, and condition keys for Amazon WorkSpaces \(p. 1916\)](#)
- [Actions, resources, and condition keys for Amazon WorkSpaces Application Manager \(p. 1922\)](#)
- [Actions, resources, and condition keys for Amazon WorkSpaces Web \(p. 1923\)](#)
- [Actions, resources, and condition keys for AWS X-Ray \(p. 1928\)](#)

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 \(p. 10\)](#)
- [Resource types defined by AWS Account Management \(p. 11\)](#)
- [Condition keys for AWS Account Management \(p. 11\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAlternateContact	Grants permission to delete the alternate contacts for an account	Write	account (p. 11)		
			accountInOrganization (p. 11)		
				account:AlternateContactTypes (p. 12)	
DisableRegion	Grants permission to disable use of a Region	Write		account:TargetRegion (p. 12)	
EnableRegion	Grants permission to enable use of a Region	Write		account:TargetRegion (p. 12)	
GetAlternateContact	Grants permission to retrieve the alternate contacts for an account	Read	account (p. 11)		
			accountInOrganization (p. 11)		
				account:AlternateContactTypes (p. 12)	
ListRegions	Grants permission to list the available Regions	List			
PutAlternateContact	Grants permission to modify the alternate contacts for an account	Write	account (p. 11)		
			accountInOrganization (p. 11)		
				account:AlternateContactTypes (p. 12)	

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 \(p. 10\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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 [Available global condition keys](#).

Condition keys	Description	Type
account:AccountResourcePaths	Filters access by the resource path for an account in an organization	ArrayOfString
account:AccountResourceTags/ \${TagKey}	Filters access by resource tags for an account in an organization	ArrayOfString
account:AlternateContactTypes	Filters access by alternate contact types	ArrayOfString
account:TargetRegions	Filters access by a list of Regions. Enables or disables all the Regions specified here	String

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 \(p. 12\)](#)
- [Resource types defined by AWS Activate \(p. 13\)](#)
- [Condition keys for AWS Activate \(p. 13\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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			
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 [Available keys for conditions](#).

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:

- View a list of the [API operations available for this service](#).

Topics

- [Actions defined by Alexa for Business \(p. 14\)](#)

- [Resource types defined by Alexa for Business \(p. 21\)](#)
- [Condition keys for Alexa for Business \(p. 22\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 21)		
			contact* (p. 21)		
AssociateDeviceWithDeviceProfile	Grants permission to associate a device with the specified network profile	Write	device* (p. 21)		
			networkprofile* (p. 22)		
AssociateDeviceWithRoom	Grants permission to associate a device with given room	Write	device* (p. 21)		
			room* (p. 21)		
AssociateSkillGroupWithSkillGroup	Grants permission to associate the skill group with given room	Write	room* (p. 21)		
			skillgroup* (p. 21)		
AssociateSkillWithSkillGroup	Grants permission to associate a skill with a skill group	Write	skillgroup* (p. 21)		
AssociateSkillWithUser	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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAddressBook	Grants permission to create an address book with the specified details	Write			
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			
CreateConferenceProvider	Grants permission to add a new conference provider under the user's AWS account	Write			
CreateContact	Grants permission to create a contact with the specified details	Write			
CreateGatewayGroup	Grants permission to create a gateway group with the specified details	Write			
CreateNetworkProfile	Grants permission to create a network profile with the specified details	Write			
CreateProfile	Grants permission to create a new profile	Write			
CreateRoom	Grants permission to create room with the specified details	Write	profile* (p. 21)		
CreateSkillGroup	Grants permission to create a skill group with given name and description	Write			
CreateUser	Grants permission to create a user	Write	user* (p. 21)		
DeleteAddressBook	Grants permission to delete an address book by the address book ARN	Write	addressbook* (p. 21)		
DeleteBusinessReportSchedule	Grants permission to delete the recurring report delivery schedule with the specified schedule ARN	Write	schedule* (p. 22)		
DeleteConferenceProvider	Grants permission to delete a conference provider	Write	conferenceprovider* (p. 21)		
DeleteContact	Grants permission to delete a contact by the contact ARN	Write	contact* (p. 21)		
DeleteDevice	Grants permission to remove a device from Alexa For Business	Write	device* (p. 21)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteDeviceUsage	Grants permission to delete the device's entire previous history of voice input data and associated response data	Write	device* (p. 21)		
DeleteGatewayGroup	Grants permission to delete a gateway group	Write	gatewaygroup* (p. 22)		
DeleteNetworkProfile	Grants permission to delete a network profile by the network profile ARN	Write	networkprofile* (p. 22)		
DeleteProfile	Grants permission to delete profile by profile ARN	Write	profile* (p. 21)		
DeleteRoom	Grants permission to delete room	Write	room* (p. 21)		
DeleteRoomSkillParameter	Grants permission to delete a parameter from a skill and room	Write	room* (p. 21)		
DeleteSkillAuthorizations	Grants permission to unlink a third party account from a skill	Write	room* (p. 21)		
DeleteSkillGroup	Grants permission to delete skill group with skill group ARN	Write	skillgroup* (p. 21)		
DeleteUser	Grants permission to delete a user	Write	user* (p. 21)		
DisassociateContact	Grants permission to disassociate a contact from a given address book	Write	addressbook* (p. 21)		
			contact* (p. 21)		
DisassociateDevice	Grants permission to disassociate device from its current room	Write	device* (p. 21)		
DisassociateSkill	Grants permission to disassociate skill from a skill group	Write	skillgroup* (p. 21)		
DisassociateSkillFromPrivate	Grants permission to make a private skill unavailable for enrolled users and prevent them from enabling it on their devices	Write	user* (p. 21)		
DisassociateSkillFromRoom	Grants permission to disassociate the skill group from given room	Write	room* (p. 21)		
			skillgroup* (p. 21)		
ForgetSmartHomeAppliances	Grants permission to forget smart home appliances associated to a room	Write	room* (p. 21)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAddressBook	Grants permission to get the address book details by the address book ARN	Read	addressbook* (p. 21)		
GetConferencePreference	Grants permission to retrieve the existing conference preferences	Read			
GetConferenceProvider	Grants permission to get details about a specific conference provider	Read	conferenceprovider* (p. 21)		
GetContact	Grants permission to get the contact details by the contact ARN	Read	contact* (p. 21)		
GetDevice	Grants permission to get device details	Read	device* (p. 21)		
GetGateway	Grants permission to retrieve the details of a gateway	Read	gateway* (p. 22)		
GetGatewayGroup	Grants permission to retrieve the details of a gateway group	Read	gatewaygroup* (p. 22)		
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* (p. 22)		
GetProfile	Grants permission to get profile when provided with Profile ARN	Read	profile* (p. 21)		
GetRoom	Grants permission to get room details	Read	room* (p. 21)		
GetRoomSkillParameter	Grants permission to get an existing parameter that has been set for a skill and room	Read	room* (p. 21)		
GetSkillGroup	Grants permission to get skill group details with skill group ARN	Read	skillgroup* (p. 21)		
ListBusinessReportDetails	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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDeviceEvents	Grants permission to list the device event history, including device connection status, for up to 30 days	List	device* (p. 21)		
ListGatewayGroups	Grants permission to list gateway group summaries	List			
ListGateways	Grants permission to list gateway summaries	List	gatewaygroup* (p. 22)		
ListSkills	Grants permission to list skills	List			
ListSkillsStoreCategories	Grants permission to list all categories in the Alexa skill store	List			
ListSkillsStoreSkillsByCategory	Grants permission to list all Alexa skill store by category	List			
ListSmartHomeAppliances	Grants permission to list all of the smart home appliances associated with a room	List	room* (p. 21)		
ListTags	Grants permission to list all tags on a resource	Read	device (p. 21)		
			room (p. 21)		
			user (p. 21)		
PutConferencePreferences	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			
PutRoomSkillParameters	Grants permission to put a room specific parameter for a skill	Write	room* (p. 21)		
PutSkillAuthorization	Grants permission to link a user's account to a third-party skill provider	Write	room* (p. 21)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterAVSDevice	Grants permission to register an Alexa-enabled device built by an Original Equipment Manufacturer (OEM) using Alexa Voice Service (AVS)	Write			
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* (p. 21)		
SearchAddressBooks	Grants permission to search address books and list the ones that meet a set of filter and sort criteria	List			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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* (p. 21)		
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			
StartSmartHomeDiscovery	Grants permission to initiate the discovery of smart home appliances associated with the room	Read	room* (p. 21)		
TagResource	Grants permission to add metadata tags to a resource	Tagging	device (p. 21)		
			room (p. 21)		
			user (p. 21)		
UntagResource	Grants permission to remove metadata tags from a resource	Tagging	device (p. 21)		
			room (p. 21)		
			user (p. 21)		
UpdateAddressBook	Grants permission to update address book details by the address book ARN	Write	addressbook* (p. 21)		
UpdateBusinessReportConfiguration	Grants permission to update the configuration of the report delivery schedule with the specified schedule ARN	Write	schedule* (p. 22)		
UpdateConferenceProvider	Grants permission to update an existing conference provider's settings	Write	conferenceprovider* (p. 21)		
UpdateContact	Grants permission to update the contact details by the contact ARN	Write	contact* (p. 21)		
UpdateDevice	Grants permission to update device name	Write	device* (p. 21)		
UpdateGateway	Grants permission to update the details of a gateway	Write	gateway* (p. 22)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateGatewayGroup	Grants permission to update the details of a gateway group	Write	gatewaygroup* (p. 22)		
UpdateNetworkProfile	Grants permission to update a network profile by the network profile ARN	Write	networkprofile* (p. 22)		
UpdateProfile	Grants permission to update an existing profile	Write	profile* (p. 21)		
UpdateRoom	Grants permission to update room details	Write	room* (p. 21)		
UpdateSkillGroup	Grants permission to update skill group details with skill group ARN	Write	skillgroup* (p. 21)		

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 \(p. 14\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
profile	<code>arn:\${Partition}:a4b:\${Region}: \${Account}:profile/\${Resource_id}</code>	
room	<code>arn:\${Partition}:a4b:\${Region}: \${Account}:room/\${Resource_id}</code>	aws:ResourceTag/\${TagKey} (p. 22)
device	<code>arn:\${Partition}:a4b:\${Region}: \${Account}:device/\${Resource_id}</code>	aws:ResourceTag/\${TagKey} (p. 22)
skillgroup	<code>arn:\${Partition}:a4b:\${Region}: \${Account}:skill-group/\${Resource_id}</code>	
user	<code>arn:\${Partition}:a4b:\${Region}: \${Account}:user/\${Resource_id}</code>	aws:ResourceTag/\${TagKey} (p. 22)
addressbook	<code>arn:\${Partition}:a4b:\${Region}: \${Account}:address-book/\${Resource_id}</code>	
conferenceprovider	<code>arn:\${Partition}:a4b:\${Region}: \${Account}:conference-provider/ \${Resource_id}</code>	
contact	<code>arn:\${Partition}:a4b:\${Region}: \${Account}:contact/\${Resource_id}</code>	

Resource types	ARN	Condition keys
schedule	arn:\${Partition}:a4b:\${Region}: \${Account}:schedule/\${Resource_id}	
networkprofile	arn:\${Partition}:a4b:\${Region}: \${Account}:network-profile/\${Resource_id}	
gateway	arn:\${Partition}:a4b:\${Region}: \${Account}:gateway/\${Resource_id}	
gatewaygroup	arn:\${Partition}:a4b:\${Region}: \${Account}:gateway-group/\${Resource_id}	

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 [Available global condition keys](#).

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

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 \(p. 23\)](#)

- Resource types defined by AmazonMediaImport (p. 23)
- Condition keys for AmazonMediaImport (p. 23)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDatabase[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 [Available keys for conditions](#).

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 \(p. 24\)](#)
- [Resource types defined by AWS Amplify \(p. 27\)](#)
- [Condition keys for AWS Amplify \(p. 27\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateApp	Creates a new Amplify App	Write	apps* (p. 27)		
			aws:RequestTag/ \${TagKey} (p. 27)		
			aws:TagKeys (p. 27)		
CreateBackendEnvironment	Creates a new backend environment for an Amplify App	Write	apps* (p. 27)		
CreateBranch	Creates a new Branch for an Amplify App	Write	apps* (p. 27)		
			aws:RequestTag/ \${TagKey} (p. 27)		
			aws:TagKeys (p. 27)		
CreateDeployment	Create a deployment for manual deploy apps. (Apps are not connected to repository)	Write	branches* (p. 27)		
CreateDomainAssociation	Create a new DomainAssociation on an App	Write	apps* (p. 27)		
			aws:RequestTag/ \${TagKey} (p. 27)		
			aws:TagKeys (p. 27)		
CreateWebHook	Create a new webhook on an App	Write	branches* (p. 27)		

Service Authorization Reference
Service Authorization Reference
AWS Amplify

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteApp	Delete an existing Amplify App by appId	Write	apps* (p. 27)		
DeleteBackendEnvironment	Deletes a branch for an Amplify App	Write	apps* (p. 27)		
DeleteBranch	Deletes a branch for an Amplify App	Write	branches* (p. 27)		
DeleteDomainAssociation	Deletes a DomainAssociation	Write	domains* (p. 27)		
DeleteJob	Delete a job, for an Amplify branch, part of Amplify App	Write	jobs* (p. 27)		
DeleteWebHook	Delete a webhook by id	Write	apps* (p. 27)		
GenerateAccessLogs	Generate website access logs for specific time range via a pre-signed URL	Write	apps* (p. 27)		
GetApp	Retrieves an existing Amplify App by appId	Read	apps* (p. 27)		
GetArtifactUrl	Retrieves artifact info that corresponds to a artifactId	Read	apps* (p. 27)		
GetBackendEnvironment	Retrieves a backend environment for an Amplify App	Read	apps* (p. 27)		
GetBranch	Retrieves a branch for an Amplify App	Read	branches* (p. 27)		
GetDomainAssociation	Retrieves domain info that corresponds to an appId and domainName	Read	domains* (p. 27)		
GetJob	Get a job for a branch, part of an Amplify App	Read	jobs* (p. 27)		
GetWebHook	Retrieves webhook info that corresponds to a webhookId	Read	apps* (p. 27)		
ListApps	Lists existing Amplify Apps	List			
ListArtifacts	List artifacts with an app, a branch, a job and an artifact type	List	apps* (p. 27)		
ListBackendEnvironments	Lists backend environments for an Amplify App	List	apps* (p. 27)		
ListBranches	Lists branches for an Amplify App	List	apps* (p. 27)		

Service Authorization Reference
Service Authorization Reference
AWS Amplify

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDomainAssociations	List domains with an app	List	apps* (p. 27)		
ListJobs	List Jobs for a branch, part of an Amplify App	List	branches* (p. 27)		
ListTagsForResource Console resource	List tags for an AWS Amplify Console resource	Read	apps (p. 27)		
			branches (p. 27)		
			jobs (p. 27)		
ListWebHooks	List webhooks on an App	List	apps* (p. 27)		
StartDeployment	Start a deployment for manual deploy apps. (Apps are not connected to repository)	Write	branches* (p. 27)		
StartJob	Starts a new job for a branch, part of an Amplify App	Write	jobs* (p. 27)		
StopJob	Stop a job that is in progress, for an Amplify branch, part of Amplify App	Write	jobs* (p. 27)		
TagResource	This action tags an AWS Amplify Console resource	Tagging	apps (p. 27)		
			branches (p. 27)		
			jobs (p. 27)		
				aws:TagKeys (p. 27)	
				aws:RequestTag/ \${TagKey} (p. 27)	
UntagResource	This action removes a tag from an AWS Amplify Console resource	Tagging	apps (p. 27)		
			branches (p. 27)		
			jobs (p. 27)		
				aws:TagKeys (p. 27)	
UpdateApp	Updates an existing Amplify App	Write	apps* (p. 27)		
UpdateBranch	Updates a branch for an Amplify App	Write	branches* (p. 27)		
UpdateDomainAssociation on App	Update a DomainAssociation on an App	Write	domains* (p. 27)		
UpdateWebHook	Update a webhook	Write	apps* (p. 27)		

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 \(p. 24\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
apps	<code>arn:\${Partition}:amplify:\${Region}: \${Account}:apps/\${AppId}</code>	aws:ResourceTag/\${TagKey} (p. 27)
branches	<code>arn:\${Partition}:amplify:\${Region}: \${Account}:apps/\${AppId}/branches/ \${BranchName}</code>	aws:ResourceTag/\${TagKey} (p. 27)
jobs	<code>arn:\${Partition}:amplify:\${Region}: \${Account}:apps/\${AppId}/branches/ \${BranchName}/jobs/\${JobId}</code>	
domains	<code>arn:\${Partition}:amplify:\${Region}: \${Account}:apps/\${AppId}/domains/ \${DomainName}</code>	aws:ResourceTag/\${TagKey} (p. 27)

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters access by a tag's key and value in a request	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters actions based on the presence of tag key-value pairs in the request	String
<code>aws:TagKeys</code>	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 \(p. 28\)](#)
- [Resource types defined by AWS Amplify Admin \(p. 31\)](#)
- [Condition keys for AWS Amplify Admin \(p. 32\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 environment	Write	backend* (p. 31)		
CreateBackend	Grants permission to create a new Amplify Admin backend environment by Amplify appId	Write	backend* (p. 31)		
CreateBackendAPI	Grants permission to create an API for an existing Amplify Admin backend environment by appId and backendEnvironmentName	Write	api* (p. 31)		
			backend* (p. 31)		
			environment* (p. 31)		
CreateBackendAuth	Grants permission to create an auth resource for an existing Amplify Admin backend environment by appId and backendEnvironmentName	Write	auth* (p. 31)		
			backend* (p. 31)		
			environment* (p. 31)		
CreateBackendConfig	Grants permission to create a config Amplify Admin backend config by Amplify appId	Write	backend* (p. 31)		
CreateBackendStorage	Grants permission to create a storage backend storage resource	Write	backend* (p. 31)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			environment* (p. 31)		
CreateToken	Grants permission to create an Amplify Admin challenge token by appId	Write	backend* (p. 31)		
DeleteBackend	Grants permission to delete an existing Amplify Admin backend environment by appId and backendEnvironmentName	Write	backend* (p. 31)		
			environment* (p. 31)		
DeleteBackendAPI	Grants permission to delete an API of an existing Amplify Admin backend environment by appId and backendEnvironmentName	Write	api* (p. 31)		
			backend* (p. 31)		
			environment* (p. 31)		
DeleteBackendAuth	Grants permission to delete an auth resource of an existing Amplify Admin backend environment by appId and backendEnvironmentName	Write	auth* (p. 31)		
			backend* (p. 31)		
			environment* (p. 31)		
DeleteBackendStorage	Grants permission to delete a backend storage resource	Write	backend* (p. 31)		
			environment* (p. 31)		
			storage* (p. 32)		
DeleteToken	Grants permission to delete an Amplify Admin challenge token by appId	Write	backend* (p. 31)		
GenerateBackendAPIModelsFor	Grants permission to generate models for an API of an existing Amplify Admin backend environment by appId and backendEnvironmentName	Write	api* (p. 31)		
			backend* (p. 31)		
			environment* (p. 31)		
GetBackend	Grants permission to retrieve an existing Amplify Admin backend environment by appId and backendEnvironmentName	Read	backend* (p. 31)		
			environment* (p. 31)		
GetBackendAPI	Grants permission to retrieve an API of an existing Amplify Admin backend environment by appId and backendEnvironmentName	Read	api* (p. 31)		
			backend* (p. 31)		
			environment* (p. 31)		
GetBackendAPIModelsFor	Grants permission to retrieve models for an API of an existing Amplify Admin backend environment by appId and backendEnvironmentName	Read	api* (p. 31)		
			backend* (p. 31)		
			environment* (p. 31)		

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* (p. 31)		
	backend* (p. 31)				
	environment* (p. 31)				
GetBackendJob	Grants permission to retrieve a job of an existing Amplify Admin backend environment by appId and backendEnvironmentName	Read	backend* (p. 31)		
	job* (p. 31)				
GetBackendStorage	Grants permission to retrieve an existing backend storage resource	Read	backend* (p. 31)		
	environment* (p. 31)				
GetToken	Grants permission to retrieve an Amplify Admin challenge token by appId	Read	backend* (p. 31)		
ImportBackendAuth	Grants permission to import an existing auth resource of an Amplify Admin backend environment by appId and backendEnvironmentName	Write	auth* (p. 31)		
	backend* (p. 31)				
	environment* (p. 31)				
ImportBackendStorage	Grants permission to import an existing backend storage resource	Write	backend* (p. 31)		
	environment* (p. 31)				
	storage* (p. 32)				
ListBackendJobs	Grants permission to retrieve the jobs of an existing Amplify Admin backend environment by appId and backendEnvironmentName	List	backend* (p. 31)		
	job* (p. 31)				
ListS3Buckets	Grants permission to retrieve s3 buckets	List			
RemoveAllBackendEnvironments	Grants permission to delete all existing Amplify Admin backend environments by appId	Write	backend* (p. 31)		
	environment* (p. 31)				
RemoveBackendConfig	Grants permission to delete an Amplify Admin backend config by Amplify appId	Write	backend* (p. 31)		
UpdateBackendAPI	Grants permission to update an API of an existing Amplify Admin backend environment by appId and backendEnvironmentName	Write	api* (p. 31)		
	backend* (p. 31)				
	environment* (p. 31)				

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateBackendAuth	Grants permission to update an auth resource of an existing Amplify Admin backend environment by appId and backendEnvironmentName	Write	auth* (p. 31)		
UpdateBackendConfig	Grants permission to update an Amplify Admin backend config by Amplify appId		backend* (p. 31)		
UpdateBackendJob	Grants permission to update a job of an existing Amplify Admin backend environment by appId and backendEnvironmentName		backend* (p. 31)	job* (p. 31)	
UpdateBackendStorage	Grants permission to update a storage resource	Write	backend* (p. 31)	environment* (p. 31)	
			storage* (p. 32)		

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 \(p. 28\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

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}/token	

Resource types	ARN	Condition keys
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 [Available keys for conditions](#).

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 \(p. 32\)](#)
- [Resource types defined by AWS Amplify UI Builder \(p. 34\)](#)
- [Condition keys for AWS Amplify UI Builder \(p. 34\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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} (p. 35) aws:TagKeys (p. 35)	
CreateTheme	Grants permission to create a theme	Write		aws:RequestTag/\${TagKey} (p. 35) aws:TagKeys (p. 35)	
DeleteComponent	Grants permission to delete a component	Write	ComponentResource* (p. 34)		
DeleteTheme	Grants permission to delete a theme	Write	ThemeResource* (p. 34)		
ExchangeCodeForToken	Grants permission to exchange a code for a token	Write			
ExportComponent	Grants permission to export components	Read			
ExportThemes	Grants permission to export themes	Read			
GetComponent	Grants permission to get an existing component	Read	ComponentResource* (p. 34)		
GetTheme	Grants permission to get an existing theme	Read	ThemeResource* (p. 34)		
ListComponents	Grants permission to list the components for an app	List			
ListTagsForResource	Grants permission to list the tags for a resource	Read	ComponentResource (p. 34) ThemeResource (p. 34)		
ListThemes	Grants permission to list the themes for an app	List			
RefreshToken	Grants permission to refresh an access token	Write			
TagResource	Grants permission to tag a resource	Tagging	ComponentResource (p. 34)		
			ThemeResource (p. 34)		
			aws:TagKeys (p. 35) aws:RequestTag/\${TagKey} (p. 35)		
UntagResource	Grants permission to untag a resource	Tagging	ComponentResource (p. 34) ThemeResource (p. 34)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys (p. 35)	
UpdateComponent	Grants permission to update a component	Write	ComponentResource* (p. 34)		
UpdateTheme	Grants permission to update a theme	Write	ThemeResource* (p. 34)		

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 \(p. 32\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
ComponentResource	arn:\${Partition}:amplifyuibuilder:\${Region}:\${Account}:app/\${AppId}/environment/\${EnvironmentName}/components/\${Id}	amplifyuibuilder:AppId (p. 34) amplifyuibuilder:ComponentsId (p. 35) amplifyuibuilder:EnvironmentName (p. 35) aws:ResourceTag/\${TagKey} (p. 35)
ThemeResource	arn:\${Partition}:amplifyuibuilder:\${Region}:\${Account}:app/\${AppId}/environment/\${EnvironmentName}/themes/\${Id}	amplifyuibuilder:AppId (p. 34) amplifyuibuilder:EnvironmentName (p. 35) amplifyuibuilder:ThemesId (p. 35) aws:ResourceTag/\${TagKey} (p. 35)

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 [Available global condition keys](#).

Condition keys	Description	Type
amplifyuibuilder:AppId	Filters access by the app ID	String

Condition keys	Description	Type
amplifyuibuilder:ComponentsId	Filters access by the component ID	String
amplifyuibuilder:EnvironmentName	Filters access by the backend environment name	String
amplifyuibuilder:ThemesId	Filters access by the theme ID	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 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 \(p. 35\)](#)
- [Resource types defined by Apache Kafka APIs for Amazon MSK clusters \(p. 38\)](#)
- [Condition keys for Apache Kafka APIs for Amazon MSK clusters \(p. 38\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 38)		kafka-cluster:Connect kafka-cluster:DescribeCluster
AlterClusterDynamic	Grants permission to alter the dynamic configuration of a cluster, equivalent to Apache Kafka's ALTER_CONFIGS CLUSTER ACL	Write	cluster* (p. 38)		kafka-cluster:Connect kafka-cluster:DescribeClusterDynamic
AlterGroup	Grants permission to join groups on a cluster, equivalent to Apache Kafka's READ GROUP ACL	Write	group* (p. 38)		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* (p. 38)		kafka-cluster:Connect kafka-cluster:DescribeTopic
AlterTopicDynamic	Grants permission to alter the dynamic configuration of topics on a cluster, equivalent to Apache Kafka's ALTER_CONFIGS TOPIC ACL	Write	topic* (p. 38)		kafka-cluster:Connect kafka-cluster:DescribeTopicDynamic
AlterTransactionalId	Grants permission to alter transactional IDs on a cluster, equivalent to Apache Kafka's WRITE TRANSACTIONAL_ID ACL	Write	transactional-id* (p. 38)		kafka-cluster:Connect kafka-cluster:DescribeTransactions kafka-cluster:WriteData
Connect	Grants permission to connect and authenticate to the cluster	Write	cluster* (p. 38)		
CreateTopic	Grants permission to create topics on a cluster, equivalent to Apache Kafka's CREATE CLUSTER/TOPIC ACL	Write	topic* (p. 38)		kafka-cluster:Connect
DeleteGroup	Grants permission to delete groups on a cluster, equivalent to Apache Kafka's DELETE GROUP ACL	Write	group* (p. 38)		kafka-cluster:Connect kafka-cluster:DescribeGroup

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTopic	Grants permission to delete topics on a cluster, equivalent to Apache Kafka's DELETE TOPIC ACL	Write	topic* (p. 38)		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* (p. 38)		kafka-cluster:Connect
DescribeClusterDyn	Grants permission to describe the dynamic configuration of a cluster, equivalent to Apache Kafka's DESCRIBE_CONFIGS CLUSTER ACL	List	cluster* (p. 38)		kafka-cluster:Connect
DescribeGroup	Grants permission to describe groups on a cluster, equivalent to Apache Kafka's DESCRIBE GROUP ACL	List	group* (p. 38)		kafka-cluster:Connect
DescribeTopic	Grants permission to describe topics on a cluster, equivalent to Apache Kafka's DESCRIBE TOPIC ACL	List	topic* (p. 38)		kafka-cluster:Connect
DescribeTopicDyn	Grants permission to describe the dynamic configuration of topics on a cluster, equivalent to Apache Kafka's DESCRIBE_CONFIGS TOPIC ACL	List	topic* (p. 38)		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* (p. 38)		kafka-cluster:Connect
ReadData	Grants permission to read data from topics on a cluster, equivalent to Apache Kafka's READ TOPIC ACL	Read	topic* (p. 38)		kafka-cluster:AlterGroup kafka-cluster:Connect kafka-cluster:DescribeTopic
WriteData	Grants permission to write data to topics on a cluster, equivalent to Apache Kafka's WRITE TOPIC ACL	Write	topic* (p. 38)		kafka-cluster:Connect kafka-cluster:DescribeTopic

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
WriteData dataIdempotentWrite	Grants permission to write data idempotently on a cluster, equivalent to Apache Kafka's IDEMPOTENT_WRITE CLUSTER ACL	Write	cluster* (p. 38)		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 \(p. 35\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 38)
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 [Available global condition 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 \(p. 39\)](#)
- [Resource types defined by Amazon API Gateway \(p. 40\)](#)
- [Condition keys for Amazon API Gateway \(p. 40\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
InvalidateCache	Used to invalidate API cache upon a client request	Write	execute-api-general* (p. 40)		
Invoke	Used to invoke an API upon a client request	Write	execute-api-general* (p. 40)		
ManageConnections	ManageConnections controls access to the @connections API	Write	execute-api-general* (p. 40)		

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 \(p. 39\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
execute-api-general	<code>arn:\${Partition}:execute-api:\${Region}:\${Account}:#\${ApiId}/#\${Stage}/\${Method}/\${ApiSpecificResourcePath}</code>	

Condition keys for Amazon API Gateway

ExecuteAPI 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 [Available keys for conditions](#).

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 \(p. 40\)](#)
- [Resource types defined by Amazon API Gateway Management \(p. 45\)](#)
- [Condition keys for Amazon API Gateway Management \(p. 51\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddCertificateToDomainName	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 (p. 47) DomainNames (p. 47)		
DELETE	Grants permission to delete a particular resource	Write	ApiKey (p. 46) Authorizer (p. 46) BasePathMapping (p. 46) ClientCertificate (p. 46) Deployment (p. 46) DocumentationPart (p. 46) DocumentationVersion (p. 47) DomainName (p. 47) GatewayResponse (p. 47) Integration (p. 48) IntegrationResponse (p. 48) Method (p. 48) MethodResponse (p. 48) Model (p. 48) RequestValidator (p. 48) Resource (p. 48) RestApi (p. 49) Stage (p. 50) Template (p. 50) UsagePlan (p. 50) UsagePlanKey (p. 51) VpcLink (p. 51)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 53) aws:TagKeys (p. 53)	
GET	Grants permission to read a particular resource	Read	Account (p. 45) ApiKey (p. 46) ApiKeys (p. 46) Authorizer (p. 46) Authorizers (p. 46) BasePathMapping (p. 46) BasePathMappings (p. 46) ClientCertificate (p. 46) ClientCertificates (p. 46) Deployment (p. 46) Deployments (p. 46) DocumentationPart (p. 46) DocumentationParts (p. 46) DocumentationVersion (p. 47) DocumentationVersions (p. 47) DomainName (p. 47) DomainNames (p. 47) GatewayResponse (p. 47) GatewayResponses (p. 47) Integration (p. 48) IntegrationResponse (p. 48) Method (p. 48) MethodResponse (p. 48) Model (p. 48) Models (p. 48) RequestValidator (p. 48) RequestValidators (p. 48)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Resource (p. 48) Resources (p. 48) RestApi (p. 49) RestApis (p. 50) Sdk (p. 50) Stage (p. 50) Stages (p. 50) UsagePlan (p. 50) UsagePlanKey (p. 51) UsagePlanKeys (p. 51) UsagePlans (p. 51) VpcLink (p. 51) VpcLinks (p. 51)		
PATCH	Grants permission to update a particular resource	Write	Account (p. 45) ApiKey (p. 46) Authorizer (p. 46) BasePathMapping (p. 46) ClientCertificate (p. 46) Deployment (p. 46) DocumentationPart (p. 46) DocumentationVersion (p. 47) DomainName (p. 47) GatewayResponse (p. 47) Integration (p. 48) IntegrationResponse (p. 48) Method (p. 48) MethodResponse (p. 48) Model (p. 48) RequestValidator (p. 48) Resource (p. 48)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			RestApi (p. 49) Stage (p. 50) Template (p. 50) UsagePlan (p. 50) UsagePlanKey (p. 51) VpcLink (p. 51)		
POST	Grants permission to create a particular resource	Write	ApiKeys (p. 46) Authorizers (p. 46) BasePathMappings (p. 46) ClientCertificates (p. 46) Deployments (p. 46) DocumentationParts (p. 46) DocumentationVersions (p. 47) DomainNames (p. 47) GatewayResponses (p. 47) IntegrationResponse (p. 48) MethodResponse (p. 48) Models (p. 48) RequestValidators (p. 48) Resources (p. 48) RestApis (p. 50) Stages (p. 50) UsagePlanKeys (p. 51) UsagePlans (p. 51) VpcLinks (p. 51)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PUT	Grants permission to update a particular resource	Write	DocumentationPart (p. 46) GatewayResponse (p. 47) IntegrationResponse (p. 48) MethodResponse (p. 48) RestApi (p. 49)	aws:RequestTag/ \${TagKey} (p. 53) aws:TagKeys (p. 53)	
RemoveCertificate	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 (p. 47) DomainNames (p. 47)		
SetWebACL	Grants permission 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 (p. 50) Stages (p. 50)		
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 (p. 49) RestApis (p. 50)		

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 \(p. 40\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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	

Resource types	ARN	Condition keys
ApiKey	arn:\${Partition}:apigateway:\${Region}::/apikeys/\${ApiKeyID}	aws:ResourceTag/\${TagKey} (p. 53)
ApiKeys	arn:\${Partition}:apigateway:\${Region}::/apikeys	aws:ResourceTag/\${TagKey} (p. 53)
Authorizer	arn:\${Partition}:apigateway:\${Region}::/restapis/\${RestAPIID}/authorizers/\${AuthorizerID}	apigateway:Request/AuthorizerType (p. 51) apigateway:Request/AuthorizerURI (p. 51) apigateway:Resource/AuthorizerType (p. 52) apigateway:Resource/AuthorizerURI (p. 52) aws:ResourceTag/\${TagKey} (p. 53)
Authorizers	arn:\${Partition}:apigateway:\${Region}::/restapis/\${RestAPIID}/authorizers	apigateway:Request/AuthorizerType (p. 51) apigateway:Request/AuthorizerURI (p. 51) aws:ResourceTag/\${TagKey} (p. 53)
BasePathMapping	arn:\${Partition}:apigateway:\${Region}::/domainnames/\${DomainName}/basepathmappings/\${basePath}	aws:ResourceTag/\${TagKey} (p. 53)
BasePathMapping	arn:\${Partition}:apigateway:\${Region}::/domainnames/\${DomainName}/basepathmappings	aws:ResourceTag/\${TagKey} (p. 53)
ClientCertificate	arn:\${Partition}:apigateway:\${Region}::/clientcertificates/\${ClientCertificateID}	aws:ResourceTag/\${TagKey} (p. 53)
ClientCertificates	arn:\${Partition}:apigateway:\${Region}::/clientcertificates	aws:ResourceTag/\${TagKey} (p. 53)
Deployment	arn:\${Partition}:apigateway:\${Region}::/restapis/\${RestAPIID}/deployments/\${DeploymentID}	aws:ResourceTag/\${TagKey} (p. 53)
Deployments	arn:\${Partition}:apigateway:\${Region}::/restapis/\${RestAPIID}/deployments	apigateway:Request/StageName (p. 52)
DocumentationPart	arn:\${Partition}:apigateway:\${Region}::/restapis/\${RestAPIID}/documentation/parts/\${DocumentationPartID}	aws:ResourceTag/\${TagKey} (p. 53)
DocumentationPart	arn:\${Partition}:apigateway:\${Region}::/restapis/\${RestAPIID}/documentation/parts	aws:ResourceTag/\${TagKey} (p. 53)

Resource types	ARN	Condition keys
DocumentationVersion	arn:\${Partition}:apigateway:\${Region}::/ restapis/\${RestApiId}/documentation/ versions/\${DocumentationVersionId}	
DocumentationVersion	arn:\${Partition}:apigateway:\${Region}::/ restapis/\${RestApiId}/documentation/versions	
DomainName	arn:\${Partition}:apigateway:\${Region}::/ domainnames/\${DomainName}	apigateway:Request/ EndpointType (p. 52) apigateway:Request/ MtlsTrustStoreUri (p. 52) apigateway:Request/ MtlsTrustStoreVersion (p. 52) apigateway:Request/ SecurityPolicy (p. 52) apigateway:Resource/ EndpointType (p. 53) apigateway:Resource/ MtlsTrustStoreUri (p. 53) apigateway:Resource/ MtlsTrustStoreVersion (p. 53) apigateway:Resource/ SecurityPolicy (p. 53) aws:ResourceTag/ \${TagKey} (p. 53)
DomainNames	arn:\${Partition}:apigateway:\${Region}::/ domainnames	apigateway:Request/ EndpointType (p. 52) apigateway:Request/ MtlsTrustStoreUri (p. 52) apigateway:Request/ MtlsTrustStoreVersion (p. 52) apigateway:Request/ SecurityPolicy (p. 52) aws:ResourceTag/ \${TagKey} (p. 53)
GatewayResponse	arn:\${Partition}:apigateway:\${Region}::/ restapis/\${RestApiId}/gatewayresponses/ \${ResponseType}	aws:ResourceTag/ \${TagKey} (p. 53)
GatewayResponse	arn:\${Partition}:apigateway:\${Region}::/ restapis/\${RestApiId}/gatewayresponses	aws:ResourceTag/ \${TagKey} (p. 53)

Resource types	ARN	Condition keys
Integration	arn:\${Partition}:apigateway:\${Region}::/ restapis/\${RestApiId}/resources/ \${ResourceId}/methods/\${HttpMethodType}/ integration	aws:ResourceTag/\${TagKey} (p. 53)
IntegrationResponse	arn:\${Partition}:apigateway:\${Region}::/ restapis/\${RestApiId}/resources/ \${ResourceId}/methods/\${HttpMethodType}/ integration/responses/\${StatusCode}	
Method	arn:\${Partition}:apigateway:\${Region}::/ restapis/\${RestApiId}/resources/ \${ResourceId}/methods/\${HttpMethodType}	apigateway:Request/ApiKeyRequired (p. 51) apigateway:Request/RouteAuthorizationType (p. 52) apigateway:Resource/ApiKeyRequired (p. 52) apigateway:Resource/RouteAuthorizationType (p. 53) aws:ResourceTag/\${TagKey} (p. 53)
MethodResponse	arn:\${Partition}:apigateway:\${Region}::/ restapis/\${RestApiId}/resources/ \${ResourceId}/methods/\${HttpMethodType}/ responses/\${StatusCode}	
Model	arn:\${Partition}:apigateway:\${Region}::/ restapis/\${RestApiId}/models/\${ModelName}	aws:ResourceTag/\${TagKey} (p. 53)
Models	arn:\${Partition}:apigateway:\${Region}::/ restapis/\${RestApiId}/models	aws:ResourceTag/\${TagKey} (p. 53)
RequestValidator	arn:\${Partition}:apigateway:\${Region}::/ restapis/\${RestApiId}/requestvalidators/ \${RequestValidatorId}	
RequestValidators	arn:\${Partition}:apigateway:\${Region}::/ restapis/\${RestApiId}/requestvalidators	
Resource	arn:\${Partition}:apigateway:\${Region}::/ restapis/\${RestApiId}/resources/ \${ResourceId}	aws:ResourceTag/\${TagKey} (p. 53)
Resources	arn:\${Partition}:apigateway:\${Region}::/ restapis/\${RestApiId}/resources	aws:ResourceTag/\${TagKey} (p. 53)

Resource types	ARN	Condition keys
RestApi	<code>arn:\${Partition}:apigateway:\${Region}::/ restapis/\${RestApiId}</code>	apigateway:Request/ApiKeyRequired (p. 51) apigateway:Request/ApiName (p. 51) apigateway:Request/AuthorizerType (p. 51) apigateway:Request/AuthorizerUri (p. 51) apigateway:Request/DisableExecuteApiEndpoint (p. 52) apigateway:Request/EndpointType (p. 52) apigateway:Request/RouteAuthorizationType (p. 52) apigateway:Resource/ApiKeyRequired (p. 52) apigateway:Resource/ApiName (p. 52) apigateway:Resource/AuthorizerType (p. 52) apigateway:Resource/AuthorizerUri (p. 52) apigateway:Resource/DisableExecuteApiEndpoint (p. 53) apigateway:Resource/EndpointType (p. 53) apigateway:Resource/RouteAuthorizationType (p. 53) aws:ResourceTag/\${TagKey} (p. 53)

Resource types	ARN	Condition keys
RestApis	<code>arn:\${Partition}:apigateway:\${Region}::/ restapis</code>	apigateway:Request/ApiKeyRequired (p. 51) apigateway:Request/ApiName (p. 51) apigateway:Request/AuthorizerType (p. 51) apigateway:Request/AuthorizerUri (p. 51) apigateway:Request/DisableExecuteApiEndpoint (p. 52) apigateway:Request/EndpointType (p. 52) apigateway:Request/RouteAuthorizationType (p. 52) aws:ResourceTag/\${TagKey} (p. 53)
Sdk	<code>arn:\${Partition}:apigateway:\${Region}::/ restapis/\${RestApiId}/stages/\${StageName}/ sdks/\${SdkType}</code>	
Stage	<code>arn:\${Partition}:apigateway:\${Region}::/ restapis/\${RestApiId}/stages/\${StageName}</code>	apigateway:Request/AccessLoggingDestination (p. 51) apigateway:Request/AccessLoggingFormat (p. 51) apigateway:Resource/AccessLoggingDestination (p. 52) apigateway:Resource/AccessLoggingFormat (p. 52) aws:ResourceTag/\${TagKey} (p. 53)
Stages	<code>arn:\${Partition}:apigateway:\${Region}::/ restapis/\${RestApiId}/stages</code>	apigateway:Request/AccessLoggingDestination (p. 51) apigateway:Request/AccessLoggingFormat (p. 51) aws:ResourceTag/\${TagKey} (p. 53)
Template	<code>arn:\${Partition}:apigateway:\${Region}::/ restapis/models/\${ModelName}/template</code>	
UsagePlan	<code>arn:\${Partition}:apigateway:\${Region}::/ usageplans/\${UsagePlanId}</code>	aws:ResourceTag/\${TagKey} (p. 53)

Resource types	ARN	Condition keys
UsagePlans	arn:\${Partition}:apigateway:\${Region}::/usageplans	aws:ResourceTag/\${TagKey} (p. 53)
UsagePlanKey	arn:\${Partition}:apigateway:\${Region}::/usageplans/\${UsagePlanId}/keys/\${Id}	
UsagePlanKeys	arn:\${Partition}:apigateway:\${Region}::/usageplans/\${UsagePlanId}/keys	
VpcLink	arn:\${Partition}:apigateway:\${Region}::/vpclinks/\${VpcLinkId}	aws:ResourceTag/\${TagKey} (p. 53)
VpcLinks	arn:\${Partition}:apigateway:\${Region}::/vpclinks	aws:ResourceTag/\${TagKey} (p. 53)

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 [Available global condition keys](#).

Condition keys	Description	Type
AccessLoggingDestination	Filters access by access log destination. Available during the apigateway:Request/CreateStage and UpdateStage operations	String
AccessLoggingFormat	Filters access by access log format. Available during the apigateway:Request/CreateStage and UpdateStage operations	String
ApiKeyRequired	Filters access based on 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
ApiName	Filters access by API name. Available during the apigateway:Request/CreateRestApi and UpdateRestApi operations	String
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
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

Condition keys	Description	Type
<code>apigateway:Request/Available</code> <code>DisableExecuteApiEndpointOperations</code>	Filters access by status of the default execute-api endpoint.	Bool
<code>apigateway:Request/EndpointType</code>	Filters access by endpoint type. Available during the CreateDomainName, UpdateDomainName, CreateRestApi, and UpdateRestApi operations	ArrayOfString
<code>apigateway:Request/MtlsTrustStoreUri</code>	Filters access by URI of the truststore used for mutual TLS authentication. Available during the CreateDomainName and UpdateDomainName operations	String
<code>apigateway:Request/MtlsTrustStoreVersion</code>	Filters access by version of the truststore used for mutual TLS authentication. Available during the CreateDomainName and UpdateDomainName operations	String
<code>apigateway:Request/RouteAuthorizationType</code>	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
<code>apigateway:Request/SecurityPolicy</code>	Filters access by TLS version. Available during the CreateDomain and UpdateDomain operations	ArrayOfString
<code>apigateway:Request/StageName</code>	Filters access by stage name of the deployment that you attempt to create. Available during the CreateDeployment operation	String
<code>apigateway:Resource/AccessLoggingDestination</code>	Filters access by access log destination of the current Stage resource. Available during the UpdateStage and DeleteStage operations	String
<code>apigateway:Resource/AccessLoggingFormat</code>	Filters access by access log format of the current Stage resource. Available during the UpdateStage and DeleteStage operations	String
<code>apigateway:Resource/ApiKeyRequired</code>	Filters access based on 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
<code>apigateway:Resource/ApiName</code>	Filters access by API name of the existing RestApi resource. Available during UpdateRestApi and DeleteRestApi operations	String
<code>apigateway:Resource/AuthorizerType</code>	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
<code>apigateway:Resource/AuthorizerUri</code>	Filters access by URI of a Lambda authorizer function. Available during UpdateAuthorizer and DeleteAuthorizer operations. Also available during reimport as an ArrayOfString	ArrayOfString

Condition keys	Description	Type
<code>apigateway:ResourceEndpoint</code>	Filters access by status of the default execute-api endpoint of the current RestApi resource. Available during <code>DisableExecuteApiEndpoint</code> , <code>UpdateRestApi</code> and <code>DeleteRestApi</code> operations	Bool
<code>apigateway:ResourceEndpointType</code>	Filters access by endpoint type. Available during the <code>UpdateDomainName</code> , <code>DeleteDomainName</code> , <code>UpdateRestApi</code> , and <code>DeleteRestApi</code> operations	ArrayOfString
<code>apigateway:ResourceMtlsTrustStoreUri</code>	Filters access by URI of the truststore used for mutual TLS authentication. Available during <code>UpdateDomainName</code> and <code>DeleteDomainName</code> operations	String
<code>apigateway:ResourceMtlsTrustStoreVersion</code>	Filters access by version of the truststore used for mutual TLS authentication. Available during <code>UpdateDomainName</code> and <code>DeleteDomainName</code> operations	String
<code>apigateway:ResourceRouteAuthorizationType</code>	Filters access by authorization type of the existing Method resource, for example NONE, AWS_IAM, CUSTOM, JWT, COGNITO_USER_POOLS. Available during the <code>PutMethod</code> and <code>DeleteMethod</code> operations. Also available as a collection during reimport	ArrayOfString
<code>apigateway:ResourceSecurityPolicy</code>	Filters access by TLS version. Available during <code>UpdateDomain</code> and <code>DeleteDomain</code> operations	ArrayOfString
<code>aws:RequestTag/\${TagKey}</code>	Filters actions based on the presence of tag key-value pairs in the request	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters actions based on tag key-value pairs attached to the resource	String
<code>aws:TagKeys</code>	Filters actions based on the presence of tag keys in the request	String

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 \(p. 54\)](#)
- [Resource types defined by Amazon API Gateway Management V2 \(p. 56\)](#)
- [Condition keys for Amazon API Gateway Management V2 \(p. 60\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DELETE	Grants permission to delete a particular resource	Write	AccessLogSettings (p. 57) Api (p. 57) ApiMapping (p. 58) Authorizer (p. 58) AuthorizersCache (p. 58) Cors (p. 58) Deployment (p. 59) Integration (p. 59) IntegrationResponse (p. 59) Model (p. 59) Route (p. 59) RouteRequestParameter (p. 60) RouteResponse (p. 60) RouteSettings (p. 60) Stage (p. 60) aws:RequestTag/ {\$TagKey} (p. 62) aws:TagKeys (p. 63)		
GET	Grants permission to read a particular resource	Read	AccessLogSettings (p. 57) Api (p. 57)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ApiMapping (p. 58) ApiMappings (p. 58) Apis (p. 57) Authorizer (p. 58) Authorizers (p. 58) AuthorizersCache (p. 58) Cors (p. 58) Deployment (p. 59) Deployments (p. 59) ExportedAPI (p. 59) Integration (p. 59) IntegrationResponse (p. 59) IntegrationResponses (p. 59) Integrations (p. 59) Model (p. 59) ModelTemplate (p. 59) Models (p. 59) Route (p. 59) RouteRequestParameter (p. 60) RouteResponse (p. 60) RouteResponses (p. 60) RouteSettings (p. 60) Routes (p. 60) Stage (p. 60) Stages (p. 60)		
PATCH	Grants permission to update a particular resource	Write	Api (p. 57) ApiMapping (p. 58) Authorizer (p. 58) Deployment (p. 59) Integration (p. 59)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			IntegrationResponse (p. 59) Model (p. 59) Route (p. 59) RouteRequestParameter (p. 60) RouteResponse (p. 60) Stage (p. 60)		aws:RequestTag/ \${TagKey} (p. 62) aws:TagKeys (p. 63)
POST	Grants permission to create a particular resource	Write	ApiMappings (p. 58) Apis (p. 57) Authorizers (p. 58) Deployments (p. 59) IntegrationResponses (p. 59) Integrations (p. 59) Models (p. 59) RouteResponses (p. 60) Routes (p. 60) Stages (p. 60)		aws:RequestTag/ \${TagKey} (p. 62) aws:TagKeys (p. 63)
PUT	Grants permission to update a particular resource	Write	Apis (p. 57)		aws:RequestTag/ \${TagKey} (p. 62) aws:TagKeys (p. 63)

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 \(p. 54\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you

can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
AccessLogSetting	arn:\${Partition}:apigateway:\${Region}::/apis/\${ApiId}/stages/\${StageName}/accesslogsettings	
Api	arn:\${Partition}:apigateway:\${Region}::/apis/\${ApiId}	apigateway:Request/ApiKeyRequired (p. 61) apigateway:Request/ApiName (p. 61) apigateway:Request/AuthorizerType (p. 61) apigateway:Request/AuthorizerUri (p. 61) apigateway:Request/DisableExecuteApiEndpoint (p. 61) apigateway:Request/EndpointType (p. 61) apigateway:Request/RouteAuthorizationType (p. 61) apigateway:Resource/ApiKeyRequired (p. 62) apigateway:Resource/ApiName (p. 62) apigateway:Resource/AuthorizerType (p. 62) apigateway:Resource/AuthorizerUri (p. 62) apigateway:Resource/DisableExecuteApiEndpoint (p. 62) apigateway:Resource/EndpointType (p. 62) apigateway:Resource/RouteAuthorizationType (p. 62) aws:ResourceTag/\${TagKey} (p. 62)
Apis	arn:\${Partition}:apigateway:\${Region}::/apis	apigateway:Request/ApiKeyRequired (p. 61) apigateway:Request/ApiName (p. 61)

Resource types	ARN	Condition keys
		apigateway:Request/AuthorizerType (p. 61) apigateway:Request/AuthorizerUri (p. 61) apigateway:Request/DisableExecuteApiEndpoint (p. 61) apigateway:Request/EndpointType (p. 61) apigateway:Request/RouteAuthorizationType (p. 61) aws:ResourceTag/\${TagKey} (p. 62)
ApiMapping	<code>arn:\${Partition}:apigateway:\${Region}::/domainnames/\${DomainName}/apimappings/\${ApiMappingId}</code>	aws:ResourceTag/\${TagKey} (p. 62)
ApiMappings	<code>arn:\${Partition}:apigateway:\${Region}::/domainnames/\${DomainName}/apimappings</code>	aws:ResourceTag/\${TagKey} (p. 62)
Authorizer	<code>arn:\${Partition}:apigateway:\${Region}::/apis/\${ApiId}/authorizers/\${AuthorizerId}</code>	apigateway:Request/AuthorizerType (p. 61) apigateway:Request/AuthorizerUri (p. 61) apigateway:Resource/AuthorizerType (p. 62) apigateway:Resource/AuthorizerUri (p. 62) aws:ResourceTag/\${TagKey} (p. 62)
Authorizers	<code>arn:\${Partition}:apigateway:\${Region}::/apis/\${ApiId}/authorizers</code>	apigateway:Request/AuthorizerType (p. 61) apigateway:Request/AuthorizerUri (p. 61) aws:ResourceTag/\${TagKey} (p. 62)
AuthorizersCache	<code>arn:\${Partition}:apigateway:\${Region}::/apis/\${ApiId}/stages/\${StageName}/cache/authorizers</code>	
Cors	<code>arn:\${Partition}:apigateway:\${Region}::/apis/\${ApiId}/cors</code>	

Resource types	ARN	Condition keys
Deployment	arn:\${Partition}:apigateway:\${Region}::/ apis/\${ApiId}/deployments/\${DeploymentId}	aws:ResourceTag/ \${TagKey} (p. 62)
Deployments	arn:\${Partition}:apigateway:\${Region}::/ apis/\${ApiId}/deployments	apigateway:Request/ StageName (p. 61) aws:ResourceTag/ \${TagKey} (p. 62)
ExportedAPI	arn:\${Partition}:apigateway:\${Region}::/ apis/\${ApiId}/exports/\${Specification}	
Integration	arn:\${Partition}:apigateway:\${Region}::/ apis/\${ApiId}/integrations/\${IntegrationId}	aws:ResourceTag/ \${TagKey} (p. 62)
Integrations	arn:\${Partition}:apigateway:\${Region}::/ apis/\${ApiId}/integrations	aws:ResourceTag/ \${TagKey} (p. 62)
IntegrationResponse	arn:\${Partition}:apigateway: \${Region}::/apis/\${ApiId}/integrations/ \${IntegrationId}/integrationresponses/ \${IntegrationResponseId}	
IntegrationResponses	arn:\${Partition}:apigateway:\${Region}::/ apis/\${ApiId}/integrations/\${IntegrationId}/ integrationresponses	
Model	arn:\${Partition}:apigateway:\${Region}::/ apis/\${ApiId}/models/\${ModelError}	aws:ResourceTag/ \${TagKey} (p. 62)
Models	arn:\${Partition}:apigateway:\${Region}::/ apis/\${ApiId}/models	aws:ResourceTag/ \${TagKey} (p. 62)
ModelTemplate	arn:\${Partition}:apigateway:\${Region}::/ apis/\${ApiId}/models/\${ModelError}/template	
Route	arn:\${Partition}:apigateway:\${Region}::/ apis/\${ApiId}/routes/\${RouteId}	apigateway:Request/ ApiKeyRequired (p. 61) apigateway:Request/ RouteAuthorizationType (p. 61) apigateway:Resource/ ApiKeyRequired (p. 62) apigateway:Resource/ RouteAuthorizationType (p. 62) aws:ResourceTag/ \${TagKey} (p. 62)

Resource types	ARN	Condition keys
Routes	<code>arn:\${Partition}:apigateway:\${Region}::/ apis/\${ApiId}/routes</code>	apigateway:Request/ApiKeyRequired (p. 61) apigateway:Request/RouteAuthorizationType (p. 61) aws:ResourceTag/\${TagKey} (p. 62)
RouteResponse	<code>arn:\${Partition}:apigateway:\${Region}::/ apis/\${ApiId}/routes/\${RouteId}/ routeresponses/\${RouteResponseId}</code>	
RouteResponses	<code>arn:\${Partition}:apigateway:\${Region}::/ apis/\${ApiId}/routes/\${RouteId}/ routeresponses</code>	
RouteRequestParameters	<code>arn:\${Partition}:apigateway:\${Region}::/ apis/\${ApiId}/routes/\${RouteId}/ requestparameters/\${RequestParameterKey}</code>	
RouteSettings	<code>arn:\${Partition}:apigateway:\${Region}::/ apis/\${ApiId}/stages/\${StageName}/ routesettings/\${RouteKey}</code>	
Stage	<code>arn:\${Partition}:apigateway:\${Region}::/ apis/\${ApiId}/stages/\${StageName}</code>	apigateway:Request/AccessLoggingDestination (p. 61) apigateway:Request/AccessLoggingFormat (p. 61) apigateway:Resource/AccessLoggingDestination (p. 62) apigateway:Resource/AccessLoggingFormat (p. 62) aws:ResourceTag/\${TagKey} (p. 62)
Stages	<code>arn:\${Partition}:apigateway:\${Region}::/ apis/\${ApiId}/stages</code>	apigateway:Request/AccessLoggingDestination (p. 61) apigateway:Request/AccessLoggingFormat (p. 61) aws:ResourceTag/\${TagKey} (p. 62)

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 [Available global condition 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 based on whether an API key is required or not. 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/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	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/RouteAuthorizationType	Filters access by authorization type, for example NONE, AWS_IAM, CUSTOM, JWT. Available during the CreateRoute and UpdateRoute operations. Also available as a collection during import	ArrayOfString
apigateway:Request/SecurityPolicy	Filters access by TLS version. Available during the /CreateDomain and UpdateDomain operations	ArrayOfString
apigateway:Request/StageName	Filters access by stage name of the deployment that you attempt to create. Available during the CreateDeployment operation	String

Condition keys	Description	Type
<code>apigateway:Resource/AccessLoggingDestination</code>	Filters access by access log destination of the current Stage resource. Available during the UpdateStage and DeleteStage operations	String
<code>apigateway:Resource/AccessLoggingFormat</code>	Filters access by access log format of the current Stage resource. Available during the UpdateStage and DeleteStage operations	String
<code>apigateway:Resource/ApiKeyRequired</code>	Filters access based on whether an API key is required or not for the existing Route resource. Available during the UpdateRoute and DeleteRoute operations. Also available as a collection during reimport	ArrayOfBool
<code>apigateway:Resource/ApiName</code>	Filters access by API name. Available during the UpdateApi and DeleteApi operations	String
<code>apigateway:Resource/AuthorizerType</code>	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
<code>apigateway:Resource/AuthorizerUri</code>	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
<code>apigateway:Resource/DisableExecuteApiEndpoint</code>	Filters access by status of the default execute-api endpoint. Available during the UpdateApi and DeleteApi operations	Bool
<code>apigateway:Resource/EndpointType</code>	Filters access by endpoint type. Available during the UpdateDomainName, DeleteDomainName, UpdateApi, and DeleteApi operations	String
<code>apigateway:Resource/MtlsTrustStoreUri</code>	Filters access by URI of the truststore used for mutual TLS authentication. Available during the UpdateDomainName and DeleteDomainName operations	String
<code>apigateway:Resource/MtlsTrustStoreVersion</code>	Filters access by version of the truststore used for mutual TLS authentication. Available during the UpdateDomainName and DeleteDomainName operations	String
<code>apigateway:Resource/RouteAuthorizationType</code>	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
<code>apigateway:Resource/SecurityPolicy</code>	Filters access by TLS version. Available during the UpdateDomainName and DeleteDomainName operations	ArrayOfString
<code>aws:RequestTag/\${TagKey}</code>	Filters actions based on the presence of tag key-value pairs in the request	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters actions based on tag key-value pairs attached to the resource	String

Condition keys	Description	Type
aws:TagKeys	Filters actions based on the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for 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 \(p. 63\)](#)
- [Resource types defined by AWS App Mesh \(p. 67\)](#)
- [Condition keys for AWS App Mesh \(p. 68\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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*	(p. 68)	
			virtualService	(p. 67)	
				aws:TagKeys (p. 68)	
				aws:RequestTag/{TagKey} (p. 68)	

Service Authorization Reference
Service Authorization Reference
AWS App Mesh

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateMesh	Grants permission to create a service mesh	Write	mesh* (p. 67) 	aws:TagKeys (p. 68) 	aws:RequestTag/\${TagKey} (p. 68)
CreateRoute	Grants permission to create a route that is associated with a virtual router	Write	route* (p. 68) virtualNode (p. 67) 	aws:TagKeys (p. 68) aws:RequestTag/\${TagKey} (p. 68)	
CreateVirtualGateway	Grants permission to create a virtual gateway within a service mesh	Write	virtualGateway* (p. 68) 	aws:TagKeys (p. 68) aws:RequestTag/\${TagKey} (p. 68)	
CreateVirtualNode	Grants permission to create a virtual node within a service mesh	Write	virtualNode* (p. 67) virtualService (p. 67) 	aws:TagKeys (p. 68) aws:RequestTag/\${TagKey} (p. 68)	
CreateVirtualRouter	Grants permission to create a virtual router within a service mesh	Write	virtualRouter* (p. 68) 	aws:TagKeys (p. 68) aws:RequestTag/\${TagKey} (p. 68)	
CreateVirtualService	Grants permission to create a virtual service within a service mesh	Write	virtualService* (p. 67) virtualNode (p. 67) virtualRouter (p. 68) 	aws:TagKeys (p. 68) aws:RequestTag/\${TagKey} (p. 68)	
DeleteGatewayRoute	Grants permission to delete an existing gateway route	Write	gatewayRoute* (p. 68)		
DeleteMesh	Grants permission to delete an existing service mesh	Write	mesh* (p. 67)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteRoute	Grants permission to delete an existing route	Write	route* (p. 68)		
DeleteVirtualGateway	Grants permission to delete an existing virtual gateway	Write	virtualGateway* (p. 68)		
DeleteVirtualNode	Grants permission to delete an existing virtual node	Write	virtualNode* (p. 67)		
DeleteVirtualRouter	Grants permission to delete an existing virtual router	Write	virtualRouter* (p. 68)		
DeleteVirtualService	Grants permission to delete an existing virtual service	Write	virtualService* (p. 67)		
DescribeGatewayRoute	Grants permission to describe an existing gateway route	Read	gatewayRoute* (p. 68)		
DescribeMesh	Grants permission to describe an existing service mesh	Read	mesh* (p. 67)		
DescribeRoute	Grants permission to describe an existing route	Read	route* (p. 68)		
DescribeVirtualGateway	Grants permission to describe an existing virtual gateway	Read	virtualGateway* (p. 68)		
DescribeVirtualNode	Grants permission to describe an existing virtual node	Read	virtualNode* (p. 67)		
DescribeVirtualRouter	Grants permission to describe an existing virtual router	Read	virtualRouter* (p. 68)		
DescribeVirtualService	Grants permission to describe an existing virtual service	Read	virtualService* (p. 67)		
ListGatewayRoutes	Grants permission to list existing gateway routes in a service mesh	List	virtualGateway* (p. 68)		
ListMeshes	Grants permission to list existing service meshes	List			
ListRoutes	Grants permission to list existing routes in a service mesh	List	virtualRouter* (p. 68)		
ListTagsForResource	Grants permission to list the tags for an App Mesh resource	List	gatewayRoute (p. 68) mesh (p. 67) route (p. 68) virtualGateway (p. 68) virtualNode (p. 67) virtualRouter (p. 68)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			virtualService (p. 67)		
ListVirtualGateways	Grants permission to list existing virtual gateways in a service mesh	List	mesh* (p. 67)		
ListVirtualNodes	Grants permission to list existing virtual nodes	List	mesh* (p. 67)		
ListVirtualRouters	Grants permission to list existing virtual routers in a service mesh	List	mesh* (p. 67)		
ListVirtualServices	Grants permission to list existing virtual services in a service mesh	List	mesh* (p. 67)		
StreamAggregates	Grants permission to receive streamed resources for an App Mesh endpoint (VirtualNode/ VirtualGateway)	Read	virtualGateway (p. 68)		
			virtualNode (p. 67)		
TagResource	Grants permission to tag a resource with a specified resourceArn	Tagging	gatewayRoute (p. 68)		
			mesh (p. 67)		
			route (p. 68)		
			virtualGateway (p. 68)		
			virtualNode (p. 67)		
			virtualRouter (p. 68)		
			virtualService (p. 67)		
			aws:TagKeys (p. 68)		
			aws:RequestTag/ \${TagKey} (p. 68)		
UntagResource	Grants permission to delete a tag from a resource		gatewayRoute (p. 68)		
			mesh (p. 67)		
			route (p. 68)		
			virtualGateway (p. 68)		
			virtualNode (p. 67)		
			virtualRouter (p. 68)		
			virtualService (p. 67)		
			aws:TagKeys (p. 68)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateGatewayRoute	Grants permission to update an existing gateway route for a specified service mesh and virtual gateway	Write	gatewayRoute* (p. 68)		
			virtualService (p. 67)		
UpdateMesh	Grants permission to update an existing service mesh	Write	mesh* (p. 67)		
UpdateRoute	Grants permission to update an existing route for a specified service mesh and virtual router	Write	route* (p. 68)		
			virtualNode (p. 67)		
UpdateVirtualGateway	Grants permission to update an existing virtual gateway in a specified service mesh	Write	virtualGateway* (p. 68)		
UpdateVirtualNode	Grants permission to update an existing virtual node in a specified service mesh	Write	virtualNode* (p. 67)		
UpdateVirtualRouter	Grants permission to update an existing virtual router in a specified service mesh	Write	virtualRouter* (p. 68)		
UpdateVirtualService	Grants permission to update an existing virtual service in a specified service mesh	Write	virtualService* (p. 67)		
			virtualNode (p. 67)		
			virtualRouter (p. 68)		

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 \(p. 63\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 68)
virtualService	arn:\${Partition}:appmesh:\${Region}: \${Account}:mesh/\${MeshName}/virtualService/ \${VirtualServiceName}	aws:ResourceTag/ \${TagKey} (p. 68)
virtualNode	arn:\${Partition}:appmesh:\${Region}: \${Account}:mesh/\${MeshName}/virtualNode/ \${VirtualNodeName}	aws:ResourceTag/ \${TagKey} (p. 68)

Resource types	ARN	Condition keys
virtualRouter	<code>arn:\${Partition}:appmesh:\${Region}: \${Account}:mesh/\${MeshName}/virtualRouter/ \${VirtualRouterName}</code>	aws:ResourceTag/\${TagKey} (p. 68)
route	<code>arn:\${Partition}:appmesh:\${Region}: \${Account}:mesh/\${MeshName}/virtualRouter/ \${VirtualRouterName}/route/\${RouteName}</code>	aws:ResourceTag/\${TagKey} (p. 68)
virtualGateway	<code>arn:\${Partition}:appmesh:\${Region}: \${Account}:mesh/\${MeshName}/virtualGateway/ \${VirtualGatewayName}</code>	aws:ResourceTag/\${TagKey} (p. 68)
gatewayRoute	<code>arn:\${Partition}:appmesh:\${Region}: \${Account}:mesh/\${MeshName}/virtualGateway/ \${VirtualGatewayName}/gatewayRoute/ \${GatewayRouteName}</code>	aws:ResourceTag/\${TagKey} (p. 68)

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 [Available global condition 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 \(p. 69\)](#)
- [Resource types defined by AWS App Mesh Preview \(p. 71\)](#)

- Condition keys for AWS App Mesh Preview (p. 72)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 72)		
			virtualService (p. 72)		
CreateMesh	Grants permission to create a service mesh	Write	mesh* (p. 71)		
CreateRoute	Grants permission to create a route that is associated with a virtual router	Write	route* (p. 72)		
			virtualNode (p. 72)		
CreateVirtualGateway	Grants permission to create a virtual gateway within a service mesh	Write	virtualGateway* (p. 72)		
CreateVirtualNode	Grants permission to create a virtual node within a service mesh	Write	virtualNode* (p. 72)		
			virtualService (p. 72)		
CreateVirtualRouter	Grants permission to create a virtual router within a service mesh	Write	virtualRouter* (p. 72)		
CreateVirtualService	Grants permission to create a virtual service within a service mesh	Write	virtualService* (p. 72)		
			virtualNode (p. 72)		
			virtualRouter (p. 72)		
DeleteGatewayRoute	Grants permission to delete an existing gateway route	Write	gatewayRoute* (p. 72)		
DeleteMesh	Grants permission to delete an existing service mesh	Write	mesh* (p. 71)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteRoute	Grants permission to delete an existing route	Write	route* (p. 72)		
DeleteVirtualGateway	Grants permission to delete an existing virtual gateway	Write	virtualGateway* (p. 72)		
DeleteVirtualNode	Grants permission to delete an existing virtual node	Write	virtualNode* (p. 72)		
DeleteVirtualRouter	Grants permission to delete an existing virtual router	Write	virtualRouter* (p. 72)		
DeleteVirtualService	Grants permission to delete an existing virtual service	Write	virtualService* (p. 72)		
DescribeGatewayRoute	Grants permission to describe an existing gateway route	Read	gatewayRoute* (p. 72)		
DescribeMesh	Grants permission to describe an existing service mesh	Read	mesh* (p. 71)		
DescribeRoute	Grants permission to describe an existing route	Read	route* (p. 72)		
DescribeVirtualGateway	Grants permission to describe an existing virtual gateway	Read	virtualGateway* (p. 72)		
DescribeVirtualNode	Grants permission to describe an existing virtual node	Read	virtualNode* (p. 72)		
DescribeVirtualRouter	Grants permission to describe an existing virtual router	Read	virtualRouter* (p. 72)		
DescribeVirtualService	Grants permission to describe an existing virtual service	Read	virtualService* (p. 72)		
ListGatewayRoutes	Grants permission to list existing gateway routes in a service mesh	List	virtualGateway* (p. 72)		
ListMeshes	Grants permission to list existing service meshes	List			
ListRoutes	Grants permission to list existing routes in a service mesh	List	virtualRouter* (p. 72)		
ListVirtualGateways	Grants permission to list existing virtual gateways in a service mesh	List	mesh* (p. 71)		
ListVirtualNodes	Grants permission to list existing virtual nodes	List	mesh* (p. 71)		
ListVirtualRouters	Grants permission to list existing virtual routers in a service mesh	List	mesh* (p. 71)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListVirtualService	Grants permission to list existing virtual services in a service mesh	List	mesh* (p. 71)		
StreamAggregates	Grants permission to receive streamed resources for an App Mesh endpoint (VirtualNode/ VirtualGateway)	Read	virtualGateway (p. 72)		
			virtualNode (p. 72)		
UpdateGateway	Grants permission to update an existing gateway route for a specified service mesh and virtual gateway	Write	gatewayRoute* (p. 72)		
UpdateMesh	Grants permission to update an existing service mesh		mesh* (p. 71)		
UpdateRoute	Grants permission to update an existing route for a specified service mesh and virtual router	Write	route* (p. 72)		
			virtualNode (p. 72)		
UpdateVirtualGateway	Grants permission to update an existing virtual gateway in a specified service mesh	Write	virtualGateway* (p. 72)		
UpdateVirtualNode	Grants permission to update an existing virtual node in a specified service mesh	Write	virtualNode* (p. 72)		
UpdateVirtualRouter	Grants permission to update an existing virtual router in a specified service mesh	Write	virtualRouter* (p. 72)		
UpdateVirtualService	Grants permission to update an existing virtual service in a specified service mesh	Write	virtualService* (p. 72)		
			virtualNode (p. 72)		
			virtualRouter (p. 72)		

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](#) ([p. 69](#)) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
<code>mesh</code>	<code>arn:\${Partition}:appmesh-preview:\${Region}:\${Account}:mesh/\${MeshName}</code>	

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

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 [Available keys for conditions](#).

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 \(p. 73\)](#)
- [Resource types defined by AWS App Runner \(p. 76\)](#)
- [Condition keys for AWS App Runner \(p. 77\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 77)		
CreateAutoScalingConfiguration	Grants permission to create an AWS App Runner automatic scaling configuration resource	Write	autoscalingconfiguration* (p. 77)		
				aws:RequestTag/\${TagKey} (p. 77)	
				aws:TagKeys (p. 78)	
CreateConnection	Grants permission to create an AWS App Runner connection resource	Write	connection* (p. 77)		
				aws:RequestTag/\${TagKey} (p. 77)	
				aws:TagKeys (p. 78)	
CreateObservabilityConfiguration	Grants permission to create an AWS App Runner observability configuration resource	Write	observabilityconfiguration* (p. 77)		
				aws:RequestTag/\${TagKey} (p. 77)	
				aws:TagKeys (p. 78)	
CreateService	Grants permission to create an AWS App Runner service resource	Write	service* (p. 77)		
				autoscalingconfiguration (p. 77)	
				connection (p. 77)	
				observabilityconfiguration (p. 77)	
				vpcconnector (p. 77)	
				aws:RequestTag/\${TagKey} (p. 77)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					aws:TagKeys (p. 78) apprunner:ConnectionArn (p. 77) apprunner:AutoScalingConfigurationArn (p. 77) apprunner:ObservabilityConfigurationArn (p. 77) apprunner:VpcConnectorArn (p. 77)
CreateVpcConnector	Grants permission to create an AWS App Runner VPC connector resource	Write	vpcconnector* (p. 77)		
				aws:RequestTag/ \${TagKey} (p. 77)	aws:TagKeys (p. 78)
DeleteAutoScalingConfiguration	Grants permission to delete an AWS App Runner automatic scaling configuration resource	Write	autoscalingconfiguration* (p. 77)		
DeleteConnection	Grants permission to delete an AWS App Runner connection resource	Write	connection* (p. 77)		
DeleteObservabilityConfiguration	Grants permission to delete an AWS App Runner observability configuration resource	Write	observabilityconfiguration* (p. 77)		
DeleteService	Grants permission to delete an AWS App Runner service resource	Write	service* (p. 77)		
DeleteVpcConnector	Grants permission to delete an AWS App Runner VPC connector resource	Write	vpcconnector* (p. 77)		
DescribeAutoScalingConfiguration	Grants permission to retrieve the description of an AWS App Runner automatic scaling configuration resource	Read	autoscalingconfiguration* (p. 77)		
DescribeCustomDomainNames	Grants permission to retrieve the descriptions of custom domain names associated with an AWS App Runner service	Read	service* (p. 77)		
DescribeObservabilityConfiguration	Grants permission to retrieve the description of an AWS App Runner observability configuration resource	Read	observabilityconfiguration* (p. 77)		
DescribeOperation	Grants permission to retrieve the description of an operation that occurred on an AWS App Runner service	Read	service* (p. 77)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeService	Grants permission to retrieve the description of an AWS App Runner service resource	Read	service* (p. 77)		
DescribeVpcConnector	Grants permission to retrieve the description of an AWS App Runner VPC connector resource	Read	vpcconnector* (p. 77)		
DisassociateCustomDomain	Grants permission to disassociate a custom domain name from an AWS App Runner service	Write	service* (p. 77)		
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			
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* (p. 77)		
ListServices	Grants permission to retrieve a list of running AWS App Runner services in your AWS account	List			
ListTagsForResource	Grants permission to list tags associated with an AWS App Runner resource	Read	autoscalingconfiguration (p. 77)		
			connection (p. 77)		
			observabilityconfiguration (p. 77)		
			service (p. 77)		
			vpcconnector (p. 77)		
ListVpcConnectors	Grants permission to retrieve a list of AWS App Runner VPC connectors in your AWS account	List			
PauseService	Grants permission to pause an active AWS App Runner service	Write	service* (p. 77)		
ResumeService	Grants permission to resume an active AWS App Runner service	Write	service* (p. 77)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartDeployment	Grants permission to initiate a manual deployment to an AWS App Runner service	Write	service* (p. 77)		
TagResource	Grants permission to add tags to, or update tag values of, an AWS App Runner resource	Tagging	autoscalingconfiguration (p. 77) connection (p. 77) observabilityconfiguration (p. 77) service (p. 77) vpcconnector (p. 77)		aws:TagKeys (p. 78) aws:RequestTag/\${TagKey} (p. 77)
UntagResource	Grants permission to remove tags from an AWS App Runner resource	Tagging	autoscalingconfiguration (p. 77) connection (p. 77) observabilityconfiguration (p. 77) service (p. 77) vpcconnector (p. 77)		aws:TagKeys (p. 78)
UpdateService	Grants permission to update an AWS App Runner service resource	Write	service* (p. 77) autoscalingconfiguration (p. 77) connection (p. 77) observabilityconfiguration (p. 77) vpcconnector (p. 77)		apprunner:ConnectionArn (p. 77) apprunner:AutoScalingConfigurationArn apprunner:ObservabilityConfigurationArn apprunner:VpcConnectorArn (p. 77)

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 \(p. 73\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 78)
connection	arn:\${Partition}:apprunner:\${Region}: \${Account}:connection/\${ConnectionName}/ \${ConnectionId}	aws:ResourceTag/ \${TagKey} (p. 78)
autoscalingconfig	arn:\${Partition}:apprunner:\${Region}: \${Account}:autoscalingconfiguration/ \${AutoscalingConfigurationName}/ \${AutoscalingConfigurationVersion}/ \${AutoscalingConfigurationId}	aws:ResourceTag/ \${TagKey} (p. 78)
observabilityconfig	arn:\${Partition}:apprunner:\${Region}: \${Account}:observabilityconfiguration/ \${ObservabilityConfigurationName}/ \${ObservabilityConfigurationVersion}/ \${ObservabilityConfigurationId}	aws:ResourceTag/ \${TagKey} (p. 78)
vpcconnector	arn:\${Partition}:apprunner:\${Region}: \${Account}:vpcconnector/\${VpcConnectorName}/ \${VpcConnectorVersion}/ \${VpcConnectorId}	aws:ResourceTag/ \${TagKey} (p. 78)

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 [Available global condition keys](#).

Condition keys	Description	Type
apprunner:AutoScalingActionsBasedOnArn	Filters access by the CreateService and UpdateService actions based on the ARN of an associated AutoScalingConfiguration resource	ARN
apprunner:ConnectionActionsBasedOnArn	Filters access by the CreateService and UpdateService actions based on the ARN of an associated Connection resource	ARN
apprunner:ObservabilityActionsBasedOnArn	Filters access by the CreateService and UpdateService actions based on the ARN of an associated ObservabilityConfiguration resource	ARN
apprunner:VpcConnectorActionsBasedOnArn	Filters access by the CreateService and UpdateService actions based on the ARN of an associated VpcConnector resource	ARN
aws:RequestTag/\${TagKey}	Filters access by actions based on the presence of tag key-value pairs in the request	String

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

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 \(p. 78\)](#)
- [Resource types defined by AWS AppConfig \(p. 82\)](#)
- [Condition keys for AWS AppConfig \(p. 83\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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	application* (p. 83)	aws:RequestTag/\${TagKey} (p. 83)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys (p. 83)	
CreateConfiguration	Grants permission to create a configuration profile	Write	application*	(p. 83)	
			configurationprofile*	(p. 83)	
				aws:RequestTag/ \${TagKey} (p. 83)	
				aws:TagKeys (p. 83)	
CreateDeployment	Grants permission to create a deployment strategy	Write	deploymentstrategy*	(p. 83)	
				aws:RequestTag/ \${TagKey} (p. 83)	
				aws:TagKeys (p. 83)	
CreateEnvironment	Grants permission to create an environment	Write	application*	(p. 83)	
			environment*	(p. 83)	
				aws:RequestTag/ \${TagKey} (p. 83)	
				aws:TagKeys (p. 83)	
CreateHostedConfiguration	Grants permission to create a hosted configuration version	Write	application*	(p. 83)	
			configurationprofile*	(p. 83)	
			hostedconfigurationversion*	(p. 83)	
DeleteApplication	Grants permission to delete an application	Write	application*	(p. 83)	
DeleteConfiguration	Grants permission to delete a configuration profile	Write	application*	(p. 83)	
			configurationprofile*	(p. 83)	
DeleteDeployment	Grants permission to delete a deployment strategy	Write	deploymentstrategy*	(p. 83)	
DeleteEnvironment	Grants permission to delete an environment	Write	application*	(p. 83)	
			environment*	(p. 83)	
DeleteHostedConfiguration	Grants permission to delete a hosted configuration version	Write	application*	(p. 83)	
			configurationprofile*	(p. 83)	
			hostedconfigurationversion*	(p. 83)	
GetApplication	Grants permission to view details about an application	Read	application*	(p. 83)	
				aws:ResourceTag/ \${TagKey} (p. 83)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetConfiguration	Grants permission to view details about a configuration	Read	application* (p. 83)		
			configurationprofile* (p. 83)		
			environment* (p. 83)		
			aws:ResourceTag/ \${TagKey} (p. 83)		
GetConfigurationProfile	Grants permission to view details about a configuration profile	Read	application* (p. 83)		
			configurationprofile* (p. 83)		
			aws:ResourceTag/ \${TagKey} (p. 83)		
GetDeployment	Grants permission to view details about a deployment	Read	application* (p. 83)		
			deployment* (p. 83)		
			environment* (p. 83)		
			aws:ResourceTag/ \${TagKey} (p. 83)		
GetDeploymentStrategy	Grants permission to view details about a deployment strategy	Read	deploymentstrategy* (p. 83)		
			aws:ResourceTag/ \${TagKey} (p. 83)		
GetEnvironment	Grants permission to view details about an environment	Read	application* (p. 83)		
			environment* (p. 83)		
			aws:ResourceTag/ \${TagKey} (p. 83)		
GetHostedConfiguration	Grants permission to view details about a hosted configuration version	Read	application* (p. 83)		
			configurationprofile* (p. 83)		
			hostedconfigurationversion* (p. 83)		
GetLatestConfiguration	Grants permission to retrieve a deployed configuration	Read	configuration* (p. 83)		
			aws:ResourceTag/ \${TagKey} (p. 83)		
ListApplications	Grants permission to list the applications in your account	List			
ListConfigurationProfiles	Grants permission to list the configuration profiles for an application	List	application* (p. 83)		
ListDeploymentStrategies	Grants permission to list the deployment strategies for your account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDeployments	Grants permission to list the deployments for an environment	List	application* (p. 83)		
	environment* (p. 83)				
ListEnvironments	Grants permission to list the environments for an application	List	application* (p. 83)		
ListHostedConfigurations	Grants permission to list the hosted configuration versions for a configuration profile	List	application* (p. 83)		
	configurationprofile* (p. 83)				
ListTagsForResource	Grants permission to view a list of resource tags for a specified resource	Read	application (p. 83)		
	configurationprofile (p. 83)				
	deployment (p. 83)				
	deploymentstrategy (p. 83)				
	environment (p. 83)				
	aws:ResourceTag/ \${TagKey} (p. 83)				
StartConfigurationSession	Grants permission to start a configuration session	Write	configuration* (p. 83)		
	aws:ResourceTag/ \${TagKey} (p. 83)				
StartDeployment	Grants permission to initiate a deployment	Write	application* (p. 83)		
	configurationprofile* (p. 83)				
	deployment* (p. 83)				
	deploymentstrategy* (p. 83)				
	environment* (p. 83)				
	aws:RequestTag/ \${TagKey} (p. 83)				
	aws:TagKeys (p. 83)				
StopDeployment	Grants permission to stop a deployment	Write	application* (p. 83)		
	deployment* (p. 83)				
	environment* (p. 83)				
TagResource	Grants permission to tag an appconfig resource	Tagging	application (p. 83)		
	configurationprofile (p. 83)				
	deployment (p. 83)				
	deploymentstrategy (p. 83)				

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			environment (p. 83)		
UntagResource	Grants permission to untag an appconfig resource	Tagging	aws:TagKeys (p. 83)		
			aws:RequestTag/\${TagKey} (p. 83)		
			aws:ResourceTag/\${TagKey} (p. 83)		
			application (p. 83)		
			configurationprofile (p. 83)		
			deployment (p. 83)		
UpdateApplication	Grants permission to modify an application	Write	deploymentstrategy (p. 83)		
			environment (p. 83)		
UpdateConfiguration	Grants permission to modify a configuration profile	Write	aws:TagKeys (p. 83)		
			application* (p. 83)		
			configurationprofile* (p. 83)		
UpdateDeployment	Grants permission to modify a deployment strategy	Write	aws:ResourceTag/\${TagKey} (p. 83)		
			deploymentstrategy* (p. 83)		
UpdateEnvironment	Grants permission to modify an environment	Write	aws:ResourceTag/\${TagKey} (p. 83)		
			application* (p. 83)		
			environment* (p. 83)		
ValidateConfiguration	Grants permission to validate a configuration	Write	aws:ResourceTag/\${TagKey} (p. 83)		
			application* (p. 83)		
			configurationprofile* (p. 83)		

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 \(p. 78\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you

can include in a policy. These keys are displayed in the last column of the 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} (p. 83)
environment	arn:\${Partition}:appconfig:\${Region}: \${Account}:application/\${ApplicationId}/environment/\${EnvironmentId}	aws:ResourceTag/\${TagKey} (p. 83)
configurationprofile	arn:\${Partition}:appconfig: \${Region}: \${Account}:application/ \${ApplicationId}/configurationprofile/ \${ConfigurationProfileId}	aws:ResourceTag/\${TagKey} (p. 83)
deploymentstrategy	arn:\${Partition}:appconfig:\${Region}: \${Account}:deploymentstrategy/ \${DeploymentStrategyId}	aws:ResourceTag/\${TagKey} (p. 83)
deployment	arn:\${Partition}:appconfig:\${Region}: \${Account}:application/\${ApplicationId}/environment/\${EnvironmentId}/deployment/ \${DeploymentNumber}	aws:ResourceTag/\${TagKey} (p. 83)
hostedconfiguration	arn:\${Partition}:appconfig: \${Region}: \${Account}:application/ \${ApplicationId}/configurationprofile/ \${ConfigurationProfileId}/ hostedconfigurationversion/\${VersionNumber}	
configuration	arn:\${Partition}:appconfig:\${Region}: \${Account}:application/\${ApplicationId}/environment/\${EnvironmentId}/configuration/ \${ConfigurationProfileId}	aws:ResourceTag/\${TagKey} (p. 83)

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 [Available global condition 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 based on whether mandatory tags are included 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 \(p. 84\)](#)
- [Resource types defined by Amazon AppFlow \(p. 87\)](#)
- [Condition keys for Amazon AppFlow \(p. 87\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateConnectorProfile	Grants permission to create a <code>ConnectorProfile</code> to be used with Amazon AppFlow flows	Write			
CreateFlow	Grants permission to create an Amazon AppFlow flow	Write		aws:RequestTag/\${TagKey} (p. 87) aws:TagKeys (p. 87)	
DeleteConnectorProfile	Grants permission to delete a <code>ConnectorProfile</code> configured in Amazon AppFlow	Write	connectorprofile* (p. 87)		
DeleteFlow	Grants permission to delete an Amazon AppFlow flow	Write	flow* (p. 87)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 87) aws:TagKeys (p. 87)	
DescribeConnector	Grants permission to describe a connector registered in Amazon AppFlow	Read	connector* (p. 87)		
DescribeConnectorFields	Grants permission to describe all fields for an object in a login profile configured in Amazon AppFlow	Read	connectorprofile* (p. 87)		
DescribeConnectorFields[permission only]	Grants permission to describe all fields for an object in a login profile configured in Amazon AppFlow (Console Only)	Read	connectorprofile* (p. 87)		
DescribeConnectorProfiles	Grants permission to describe all 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			
DescribeFlowExecutions	Grants permission to describe all flow executions for a flow configured in Amazon AppFlow (Console Only)	Read	flow* (p. 87)		
DescribeFlowExecutions[flow]	Grants permission to describe all flow executions for a flow configured in Amazon AppFlow	Read	flow* (p. 87)		
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* (p. 87)		
ListConnectorFields[permission only]	Grants permission to list all objects for a login profile configured in Amazon AppFlow (Console Only)	Read	connectorprofile* (p. 87)		

Service Authorization Reference
Service Authorization Reference
Amazon AppFlow

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListConnectors	Grants permission to list all connectors supported in Amazon AppFlow	List	connector* (p. 87)		
ListFlows	Grants permission to list all flows configured in Amazon AppFlow	List	flow* (p. 87)		
ListTagsForResource	Grants permission to list tags for a flow	Read	flow* (p. 87)		
RegisterConnector	Grants permission to register an Amazon AppFlow connector	Write		aws:RequestTag/\${TagKey} (p. 87) aws:TagKeys (p. 87)	
RunFlow [permission only]	Grants permission to run a flow configured in Amazon AppFlow (Console Only)	Write	flow* (p. 87)		
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* (p. 87)		
StopFlow	Grants permission to deactivate a scheduled or event-triggered flow configured in Amazon AppFlow	Write	flow* (p. 87)		
TagResource	Grants permission to tag a flow	Tagging	flow* (p. 87)		
				aws:TagKeys (p. 87)	
				aws:RequestTag/\${TagKey} (p. 87)	
UnRegisterConnector	Grants permission to un-register a connector in Amazon AppFlow	Write	connector* (p. 87)		
				aws:RequestTag/\${TagKey} (p. 87)	
UntagResource	Grants permission to untag a flow	Tagging	flow* (p. 87)		
				aws:TagKeys (p. 87)	
UpdateConnectorProfile	Grants permission to update a connector profile configured in Amazon AppFlow	Write	connectorprofile* (p. 87)		
UpdateFlow	Grants permission to update a flow configured in Amazon AppFlow	Write	flow* (p. 87)		

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	connectorprofile* (p. 87)		

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 \(p. 84\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
connectorprofile	<code>arn:\${Partition}:appflow:\${Region}: \${Account}:connectorprofile/\${ProfileName}</code>	
flow	<code>arn:\${Partition}:appflow:\${Region}: \${Account}:flow/\${FlowName}</code>	aws:ResourceTag/\${TagKey} (p. 87)
connector	<code>arn:\${Partition}:appflow:\${Region}: \${Account}:connector/\${ConnectorLabel}</code>	aws:ResourceTag/\${TagKey} (p. 87)

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 [Available global condition 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 \(p. 88\)](#)
- [Resource types defined by Amazon AppIntegrations \(p. 91\)](#)
- [Condition keys for Amazon AppIntegrations \(p. 91\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDataIntegration <small>[new]</small>	Grants permission to create a <code>DataIntegration</code>	Write	data-integration*		
				aws:RequestTag/\${TagKey} (p. 91)	
				aws:TagKeys (p. 91)	
CreateDataIntegration <small>[permission only]</small>	Grants permission to create a <code>DataIntegration</code> Association	Write	data-integration*		
CreateEventIntegration <small>[new]</small>	Grants permission to create a <code>EventIntegration</code>	Write	event-integration*		
				aws:RequestTag/\${TagKey} (p. 91)	
				aws:TagKeys (p. 91)	
CreateEventIntegration	Grants permission to create an <code>EventIntegration</code> Association	Write	event-integration*		events:PutRule

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
[permission only]					events:PutTargets
DeleteDataIntegration	Grants permission to delete a DataIntegration	Write	data-integration* (p. 91)		
			aws:ResourceTag/\${TagKey} (p. 91)		
DeleteDataIntegrationAssociation [permission only]	Grants permission to delete a DataIntegration Association	Write	data-integration-association* (p. 91)		
DeleteEventIntegration	Grants permission to delete an EventIntegration	Write	event-integration* (p. 91)		
			aws:ResourceTag/\${TagKey} (p. 91)		
DeleteEventIntegrationAssociation [permission only]	Grants permission to delete an EventIntegration Association	Write	event-integration-association* (p. 91)		events:DeleteRule events>ListTargetsByRule events:RemoveTargets
GetDataIntegration	Grants permission to view details about DataIntegrations	Read	data-integration* (p. 91)		
			aws:ResourceTag/\${TagKey} (p. 91)		
GetEventIntegration	Grants permission to view details about EventIntegrations	Read	event-integration* (p. 91)		
			aws:ResourceTag/\${TagKey} (p. 91)		
ListDataIntegrationAssociations	Grants permission to list DataIntegrationAssociations	List			
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	data-integration (p. 91)		
			data-integration-association (p. 91)		

Service Authorization Reference
Service Authorization Reference
Amazon AppIntegrations

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			event-integration (p. 91)		
			event-integration-association (p. 91)		
			aws:ResourceTag/\${TagKey} (p. 91)		
TagResource	Grants permission to tag an Amazon AppIntegration resource	Tagging	data-integration (p. 91)		
			data-integration-association (p. 91)		
			event-integration (p. 91)		
			event-integration-association (p. 91)		
				aws:TagKeys (p. 91) aws:RequestTag/\${TagKey} (p. 91) aws:ResourceTag/\${TagKey} (p. 91)	
UntagResource	Grants permission to untag an Amazon AppIntegration resource	Tagging	data-integration (p. 91)		
			data-integration-association (p. 91)		
			event-integration (p. 91)		
			event-integration-association (p. 91)		
				aws:TagKeys (p. 91) aws:ResourceTag/\${TagKey} (p. 91)	
UpdateDataIntegration	Grants permission to modify a Data Integration	Write	data-integration* (p. 91)		
				aws:ResourceTag/\${TagKey} (p. 91)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateEventIntegration	Grants permission to modify an EventIntegration	Write	event-integration*	(p. 91)	
				aws:ResourceTag/ \${TagKey} (p. 91)	

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 \(p. 88\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 91)
event-integration-association	arn:\${Partition}:app-integrations:\${Region}:\${Account}:event-integration-association/\${EventIntegrationName}/\${ResourceId}	aws:ResourceTag/ \${TagKey} (p. 91)
data-integration	arn:\${Partition}:app-integrations:\${Region}:\${Account}:data-integration/\${DataIntegrationId}	aws:ResourceTag/ \${TagKey} (p. 91)
data-integration-association	arn:\${Partition}:app-integrations:\${Region}:\${Account}:data-integration-association/\${DataIntegrationId}/\${ResourceId}	aws:ResourceTag/ \${TagKey} (p. 91)

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 [Available global condition 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 \(p. 92\)](#)
- [Resource types defined by AWS Application Auto Scaling \(p. 93\)](#)
- [Condition keys for AWS Application Auto Scaling \(p. 93\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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			
DeleteScheduledAction	Grants permission to delete a scheduled action	Write			
DeregisterScalableTarget	Grants permission to deregister a scalable target	Write			
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	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	scaling activities in the specified namespace				
DescribeScalingPolicies	Grants permission to describe scaling policies or all scaling policies in the specified namespace	Read			
DescribeScheduledActions	Grants permission to describe scheduled actions or all scheduled actions in the specified namespace	Read			
PutScalingPolicy	Grants permission to create and update a scaling policy for a scalable target	Write			
PutScheduledAction	Grants permission to create and update a scheduled action for a scalable target	Write			
RegisterScalableTarget	Grants permission to register custom resources as scalable targets with Application Auto Scaling and to update configuration parameters used to manage a scalable target	Write			

Resource types defined by AWS Application Auto Scaling

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

Condition keys for AWS Application Auto Scaling

Application 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 [Available keys for conditions](#).

Actions, resources, and condition keys for AWS Application Cost Profiler Service

AWS Application Cost Profiler Service (service prefix: `application-cost-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 AWS Application Cost Profiler Service \(p. 94\)](#)
- [Resource types defined by AWS Application Cost Profiler Service \(p. 95\)](#)
- [Condition keys for AWS Application Cost Profiler Service \(p. 95\)](#)

Actions defined by AWS Application Cost Profiler 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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 the configuration with specific Application Cost Profiler Report thereby effectively disabling report generation	Write			
GetReportDefinition	Grants permission to fetch the configuration with specific Application Cost Profiler Report request	Read			
ImportApplicationUsage	Grants permission to import the application usage from S3	Write			
ListReportDefinitions	Grants permission to get a list of the different Application Cost Profiler Report configurations they have created	Read			
PutReportDefinition	Grants permission to create Application Cost Profiler Report configurations	Write			
UpdateReportDefinition	Grants permission to update an existing Application Cost Profiler Report configuration	Write			

Resource types defined by AWS Application Cost Profiler Service

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

Condition keys for AWS Application Cost Profiler Service

Application Cost Profiler 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 [Available keys for conditions](#).

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 \(p. 95\)](#)
- [Resource types defined by Application Discovery Arsenal \(p. 96\)](#)
- [Condition keys for Application Discovery Arsenal \(p. 96\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterOnPremiseAWSpro	Grants permission to register AWS-provided data collectors	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
[permission only]	to the Application Discovery Service				

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 [Available keys for conditions](#).

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 \(p. 96\)](#)
- [Resource types defined by AWS Application Discovery Service \(p. 101\)](#)
- [Condition keys for AWS Application Discovery Service \(p. 101\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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			
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			
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			
DeleteApplication	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			
DescribeAgents	Grants permission to DescribeAgents API. DescribeAgents lists agents or the Connector by ID or lists all agents/Connectors associated	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	with your user account if you did not specify an ID				
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			
DescribeContinuousExports	Grants permission to DescribeContinuousExports API. DescribeContinuousExports lists exports as specified by ID. All continuous exports associated with your user account 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			
DescribeImportTasks	Grants permission to DescribeImportTasks API. DescribeImportTasks returns an array of import tasks for your account, including status information, times, IDs, the Amazon S3 Object URL for the import file, and more	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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			
StartContinuousExport	Grants permission to StartContinuousExport API. StartContinuousExport starts the continuous flow of agent's discovered data into Amazon Athena	Write			iam:AttachRolePolicy iam:CreatePolicy iam:CreateRole iam:CreateServiceLinkedRole
StartDataCollection	Grants permission to StartDataCollectionByAgentIds API. StartDataCollectionByAgentIds instructs the specified agents or Connectors to start collecting data	Write			
StartExportTask	Grants permission to StartExportTask API. StartExportTask exports 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:AssociateConfig discovery>CreateApplication discovery>CreateTags discovery>ListConfigurations
StopContinuousExport	Grants permission to StopContinuousExport API. StopContinuousExport stops the continuous flow of agent's discovered data into Amazon Athena	Write			
StopDataCollection	Grants permission to StopDataCollection 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.

Condition keys for AWS Application Discovery Service

Application 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 [Available keys for conditions](#).

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 \(p. 102\)](#)
- [Resource types defined by AWS Application Migration Service \(p. 111\)](#)
- [Condition keys for AWS Application Migration Service \(p. 111\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("`*`") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
<code>BatchCreateVolumeSnapshotGroup</code> [permission only]	Grants permission to create volume snapshot group	Write	SourceServerResource* (p. 111)		
<code>BatchDeleteSnapshotRequest</code> [permission only]	Grants permission to batch delete snapshot request	Write			
<code>ChangeServerLifeCycleState</code> [source server]	Grants permission to change source server life cycle state	Write	SourceServerResource* (p. 111)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateReplicationConfigurationTemplate	Grants permission to create replication configuration template	Write		aws:RequestTag/ \${TagKey} (p. 112)	aws:TagKeys (p. 112)
CreateVcenterClient [permission only]	Grants permission to create vcenter client	Write		aws:RequestTag/ \${TagKey} (p. 112)	aws:TagKeys (p. 112)
DeleteJob	Grants permission to delete job	Write	JobResource* (p. 111)		
DeleteReplicationConfigurationTemplate	Grants permission to delete replication configuration template	Write	ReplicationConfigurationTemplateResource* (p. 111)		
DeleteSourceServer	Grants permission to delete source server	Write	SourceServerResource* (p. 111)		
DeleteVcenterClient	Grants permission to delete vcenter client	Write	VcenterClientResource* (p. 111)		
DescribeJobLogItems	Grants permission to describe job log items	Read	JobResource* (p. 111)		
DescribeJobs	Grants permission to describe jobs	List			
DescribeReplicationConfigurationTemplates	Grants permission to describe replication configuration templates	List			
DescribeReplicationServiceAssociations [permission only]	Grants permission to describe replication service associations	Read			
DescribeSnapshotRequests [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			
DisconnectFromSource	Grants permission to disconnect source server from service	Write	SourceServerResource* (p. 111)		
FinalizeCutover	Grants permission to finalize cutover	Write	SourceServerResource* (p. 111)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAgentCommand [permission only]	Grants permission to get agent command	Read	SourceServerResource* (p. 111)		
GetAgentConfirmedInfo [permission only]	Grants permission to get agent confirmed info	Read	SourceServerResource* (p. 111)		
GetAgentInstallationAssets [permission only]	Grants permission to get agent installation assets	Read			
GetAgentReplicationInfo [permission only]	Grants permission to get agent replication info	Read	SourceServerResource* (p. 111)		
GetAgentRuntimeConfiguration [permission only]	Grants permission to get agent runtime configuration	Read	SourceServerResource* (p. 111)		
GetAgentSnapshotredits [permission only]	Grants permission to get agent snapshot credits	Read	SourceServerResource* (p. 111)		
GetChannelCommands [permission only]	Grants permission to get channel commands	Read			
GetLaunchConfiguration	Grants permission to get launch configuration	Read	SourceServerResource* (p. 111)		
GetReplicationConfiguration	Grants permission to get replication configuration	Read	SourceServerResource* (p. 111)		
GetVcenterClientCommands [permission only]	Grants permission to get vcenter client commands	Read	VcenterClientResource* (p. 111)		
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
ListTagsForResource	Grants permission to list tags for a resource	Read			
MarkAsArchived	Grants permission to mark source server as archived	Write	SourceServerResource* (p. 111)		
NotifyAgentAuthentication [permission only]	Grants permission to notify agent authentication	Write	SourceServerResource* (p. 111)		
NotifyAgentConnection [permission only]	Grants permission to notify agent connection	Write	SourceServerResource* (p. 111)		
NotifyAgentDisconnection [permission only]	Grants permission to notify agent disconnection	Write	SourceServerResource* (p. 111)		
NotifyAgentReplicationProgress [permission only]	Grants permission to notify agent replication progress	Write	SourceServerResource* (p. 111)		
NotifyVcenterClient [permission only]	Grants permission to notify vcenter client started	Write	VcenterClientResource* (p. 111)		
RegisterAgentForMigration [permission only]	Grants permission to register agent	Write		aws:RequestTag/ \${TagKey} (p. 112)	aws:TagKeys (p. 112)
RetryDataReplication	Grants permission to retry replication	Write	SourceServerResource* (p. 111)		
SendAgentLogs [permission only]	Grants permission to send agent logs	Write	SourceServerResource* (p. 111)		
SendAgentMetrics [permission only]	Grants permission to send agent metrics	Write	SourceServerResource* (p. 111)		
SendChannelCommand [permission only]	Grants permission to send channel command	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendClientLogsForLogs [permission only]	Grants permission to send client logs	Write			
SendClientMetricsForMetrics [permission only]	Grants permission to send client metrics	Write			
SendVcenterClientLogsForVcenterClientLogs [permission only]	Grants permission to send vcenter client logs	Write	VcenterClientResource* (p. 111)		
SendVcenterClientMetricsForVcenterClientMetrics [permission only]	Grants permission to send vcenter client metrics	Write	VcenterClientResource* (p. 111)		
SendVcenterClientLogsForVcenterClientLogs [permission only]	Grants permission to send vcenter client logs	Write	VcenterClientResource* (p. 111)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions	
StartCutover	Grants permission to start cutover	Write	SourceServerResource* (p. ec2:AttachVolume ec2:AuthorizeSecurityGroup ec2:AuthorizeSecurityGroupRequest ec2>CreateLaunchTemplate ec2>CreateLaunchTemplateVersion ec2>CreateSecurityGroup ec2>CreateSnapshot ec2>CreateTags ec2>CreateVolume ec2>DeleteLaunchTemplate ec2>DeleteSnapshot ec2>DeleteVolume ec2>DescribeAccountAttributes ec2>DescribeAvailabilityZones ec2>DescribeImages ec2>DescribeInstanceAttribute ec2>DescribeInstanceState ec2>DescribeInstanceType ec2>DescribeInstances ec2>DescribeLaunchTemplate ec2>DescribeLaunchTemplateVersions ec2>DescribeSecurityGroups ec2>DescribeSnapshots ec2>DescribeSubnets ec2>DescribeVolumes ec2>DetachVolume ec2>ModifyInstanceAttribute ec2>ModifyLaunchTemplate ec2>ReportInstanceState			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:RevokeSecurityGroups ec2:RunInstances ec2:StartInstances ec2:StopInstances ec2:TerminateInstances iam:PassRole mgn>ListTagsForResource
	aws:RequestTag/\${TagKey} (p. 112) aws:TagKeys (p. 112)				
StartReplication	Grants permission to start replication	Write	SourceServerResource* (p. 111)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions	
StartTest	Grants permission to start test	Write	SourceServerResource* (p. ec2:AttachVolume ec2:AuthorizeSecurityGroup ec2:AuthorizeSecurityGroupRequest ec2>CreateLaunchTemplate ec2>CreateLaunchTemplateVersion ec2>CreateSecurityGroup ec2>CreateSnapshot ec2>CreateTags ec2>CreateVolume ec2>DeleteLaunchTemplate ec2>DeleteSnapshot ec2>DeleteVolume ec2>DescribeAccountAttributes ec2>DescribeAvailabilityZones ec2>DescribeImages ec2>DescribeInstanceAttribute ec2>DescribeInstanceState ec2>DescribeInstanceType ec2>DescribeInstances ec2>DescribeLaunchTemplateVersions ec2>DescribeLaunchTemplates ec2>DescribeSecurityGroups ec2>DescribeSnapshots ec2>DescribeSubnets ec2>DescribeVolumes ec2>DetachVolume ec2>ModifyInstanceAttribute ec2>ModifyLaunchTemplate ec2>ReportInstanceStatus			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:RevokeSecurityGroups ec2:RunInstances ec2:StartInstances ec2:StopInstances ec2:TerminateInstances iam:PassRole mgn>ListTagsForResource
	aws:RequestTag/ \${TagKey} (p. 112) aws:TagKeys (p. 112)				
TagResource	Grants permission to assign a resource tag	Tagging			aws:RequestTag/ \${TagKey} (p. 112) mgn>CreateAction (p. 112) aws:TagKeys (p. 112)
TerminateTargetInstances	Grants permission to terminate target instances	Write	SourceServerResource* (p. 111)		ec2>DeleteVolume ec2:DescribeInstances ec2:DescribeVolumes ec2:TerminateInstances
aws:RequestTag/ \${TagKey} (p. 112) aws:TagKeys (p. 112)					
UntagResource	Grants permission to untag a resource	Tagging			aws:TagKeys (p. 112)
UpdateAgentBacklog [permission only]	Grants permission to update agent backlog	Write	SourceServerResource* (p. 111)		
UpdateAgentConversionInfo [permission only]	Grants permission to update agent conversion info	Write	SourceServerResource* (p. 111)		
UpdateAgentReplicationInfo [permission only]	Grants permission to update agent replication info	Write	SourceServerResource* (p. 111)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAgentReplicationStepProperties [permission only]	Grants permission to update agent replication step properties	Write	SourceServerResource* (p. 111)		
UpdateAgentSourceProperties [permission only]	Grants permission to update agent source properties	Write	SourceServerResource* (p. 111)		
UpdateLaunchConfiguration	Grants permission to update launch configuration	Write	SourceServerResource* (p. 111)		
UpdateReplicationConfiguration	Grants permission to update replication configuration	Write	SourceServerResource* (p. 111)		
UpdateReplicationConfigurationTemplate	Grants permission to update replication configuration template	Write	ReplicationConfigurationTemplateResource* (p. 111)		
UpdateSourceServerReplicationType	Grants permission to update source server replication type	Write	SourceServerResource* (p. 111)		

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 \(p. 102\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 112)
ReplicationConfigurationTemplate	arn:\${Partition}:mgn:\${Region}: \${Account}:replica- configuration-template/ \${ReplicationConfigurationTemplateID}	aws:ResourceTag/ \${TagKey} (p. 112)
VcenterClientResource	arn:\${Partition}:mgn:\${Region}: \${Account}:vcenter-client/\${VcenterClientID}	aws:ResourceTag/ \${TagKey} (p. 112)
SourceServerResource	arn:\${Partition}:mgn:\${Region}: \${Account}:source-server/\${SourceServerID}	aws:ResourceTag/ \${TagKey} (p. 112)

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 [Available global condition 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
mgn>CreateAction	Filters access by the name of a resource-creating API action	String

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 \(p. 112\)](#)
- [Resource types defined by Amazon AppStream 2.0 \(p. 120\)](#)
- [Condition keys for Amazon AppStream 2.0 \(p. 121\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateApplication	Grants permission to associate the specified application with the fleet	Write	application* (p. 121)		
	fleet* (p. 121)				
	aws:ResourceTag/\${TagKey} (p. 121)				
AssociateApplication	Grants permission to associate the specified application to the specified entitlement	Write	stack* (p. 121)		
AssociateFleet	Grants permission to associate the specified fleet with the specified stack	Write	fleet* (p. 121)		
	stack* (p. 121)				
	aws:ResourceTag/\${TagKey} (p. 121)				
BatchAssociateUser	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* (p. 121)		
	aws:ResourceTag/\${TagKey} (p. 121)				
BatchDisassociateUser	Grants permission to disassociate the specified users from the specified stacks	Write	stack* (p. 121)		
	aws:ResourceTag/\${TagKey} (p. 121)				
CopyImage	Grants permission to copy the specified image within the same Region or to a new Region within the same AWS account	Write	image* (p. 121)		
	aws:ResourceTag/\${TagKey} (p. 121)				
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} (p. 121)	
				aws:ResourceTag/\${TagKey} (p. 121)	
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* (p. 121)		
	aws:RequestTag/\${TagKey} (p. 121)				
				aws:ResourceTag/\${TagKey} (p. 121)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					aws:TagKeys (p. 121)
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* (p. 121)		
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* (p. 121)		
			image (p. 121)		
				aws:RequestTag/ \${TagKey} (p. 121)	aws:TagKeys (p. 121)
CreateImageBuilder	Grants permission to create an image builder. An image builder is a virtual machine that is used to create an image	Write	image* (p. 121)		
			image-builder* (p. 121)		
				aws:RequestTag/ \${TagKey} (p. 121)	aws:TagKeys (p. 121)
CreateStreamingURL	Grants permission to create a URL to start an image builder streaming session	Write	image-builder* (p. 121)		
				aws:ResourceTag/ \${TagKey} (p. 121)	
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* (p. 121)		
				aws:RequestTag/ \${TagKey} (p. 121)	
					aws:TagKeys (p. 121)
CreateTemporaryURL	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* (p. 121)		
			stack* (p. 121)		
				aws:ResourceTag/ \${TagKey} (p. 121)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateUpdatedImage	Grants permission to update an existing image within customer account	Write	image* (p. 121)	aws:RequestTag/ {\$TagKey} (p. 121)	aws:ResourceTag/ {\$TagKey} (p. 121) aws:TagKeys (p. 121)
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* (p. 121)	aws:ResourceTag/ {\$TagKey} (p. 121)	
DeleteApplication	Grants permission to delete the specified application	Write	application* (p. 121)	aws:ResourceTag/ {\$TagKey} (p. 121)	
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* (p. 121)		
DeleteFleet	Grants permission to delete the specified fleet	Write	fleet* (p. 121)	aws:ResourceTag/ {\$TagKey} (p. 121)	
DeleteImage	Grants permission to delete the specified image. An image cannot be deleted when it is in use	Write	image* (p. 121)	aws:ResourceTag/ {\$TagKey} (p. 121)	
DeleteImageBuilder	Grants permission to delete the specified image builder and release capacity	Write	image-builder* (p. 121)	aws:ResourceTag/ {\$TagKey} (p. 121)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteImagePermissions	Grants permission to delete permissions for the specified private image	Write	image* (p. 121)		
			aws:ResourceTag/ \${TagKey} (p. 121)		
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* (p. 121)		
			aws:ResourceTag/ \${TagKey} (p. 121)		
DeleteUsageReport	Grants permission to disable usage report generation	Write			
DeleteUser	Grants permission to delete a user from the user pool	Write			
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	Read	app-block (p. 121)		
DescribeApplicationAssociations	Grants permission to retrieve the associations that are associated with the specified application or fleet	Read	application (p. 121) fleet (p. 121)		
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	Read	application (p. 121)		
DescribeDirectories	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	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeEntitlements	Grants permission to retrieve one or all entitlements for the specified stack	Read	stack* (p. 121)		
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	Read	fleet (p. 121)		
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	Read	image-builder (p. 121)		
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* (p. 121)		
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	Read	image (p. 121)		
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	Read	fleet* (p. 121)		
			stack* (p. 121)		
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	Read	stack (p. 121)		
DescribeUsageReports	Grants permission to retrieve a list that describes one or more usage report subscriptions	Read			
DescribeUserStackAssociations	Grants permission to retrieve a list that describes the UserStackAssociation objects	Read	stack (p. 121)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions	
DescribeUsers	Grants permission to retrieve a list that describes users in the user pool	Read				
DisableUser	Grants permission to disable the specified user in the user pool. This action does not delete the user	Write				
DisassociateApplicationFromFleet	Grants permission to disassociate the specified application from the specified fleet	Write	application* (p. 121)			
			fleet* (p. 121)			
DisassociateApplicationFromEntitlement	Grants permission to disassociate the specified application from the specified entitlement	Write	stack* (p. 121)			
DisassociateFleet	Grants permission to disassociate the specified fleet from the specified stack	Write	fleet* (p. 121)			
			stack* (p. 121)			
EnableUser	Grants permission to enable a user in the user pool	Write				
ExpireSession	Grants permission to immediately stop the specified streaming session	Write				
ListAssociatedFleets	Grants permission to retrieve the name of the fleet that is associated with the specified stack	Read	stack* (p. 121)			
ListAssociatedStacks	Grants permission to retrieve the name of the stack with which the specified fleet is associated	Read	fleet* (p. 121)			
ListEntitledApplications	Grants permission to retrieve the applications that are associated with the specified entitlement	List	stack* (p. 121)			
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				

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartFleet	Grants permission to start the specified fleet	Write	fleet* (p. 121)		
				aws:ResourceTag/ \${TagKey} (p. 121)	
StartImageBuilder	Grants permission to start the specified image builder	Write	image-builder* (p. 121)		
				aws:ResourceTag/ \${TagKey} (p. 121)	
StopFleet	Grants permission to stop the specified fleet	Write	fleet* (p. 121)		
				aws:ResourceTag/ \${TagKey} (p. 121)	
StopImageBuilder	Grants permission to stop the specified image builder	Write	image-builder* (p. 121)		
				aws:ResourceTag/ \${TagKey} (p. 121)	
Stream	Grants permission to federated users to sign in by using their existing credentials and stream applications from the specified stack	Write	stack* (p. 121)		
				appstream:userId (p. 121)	
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 (p. 121)		
			application (p. 121)		
			fleet (p. 121)		
			image (p. 121)		
			image-builder (p. 121)		
			stack (p. 121)		
			aws:RequestTag/ \${TagKey} (p. 121)		
UntagResource	Grants permission to disassociate one or more tags from the specified AppStream 2.0 resource	Tagging	aws:TagKeys (p. 121)		
			aws:ResourceTag/ \${TagKey} (p. 121)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			image (p. 121)		
			image-builder (p. 121)		
			stack (p. 121)		
			aws:TagKeys (p. 121)		
UpdateApplication	Grants permission to update the specified fields for the specified application	Write	application* (p. 121)		
			app-block (p. 121)		
			aws:ResourceTag/\${TagKey} (p. 121)		
UpdateDirectory	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* (p. 121)		
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* (p. 121)		
	image (p. 121)				
	aws:ResourceTag/\${TagKey} (p. 121)				
UpdateImagePermission	Grants permission to add or update permissions for the specified private image	Write	image* (p. 121)		
	aws:ResourceTag/\${TagKey} (p. 121)				
UpdateStack	Grants permission to update the specified fields for the specified stack	Write	stack* (p. 121)		
	aws:ResourceTag/\${TagKey} (p. 121)				

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 \(p. 112\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 121)
image	arn:\${Partition}:appstream:\${Region}: \${Account}:image/\${ImageName}	aws:ResourceTag/ \${TagKey} (p. 121)
image-builder	arn:\${Partition}:appstream:\${Region}: \${Account}:image-builder/\${ImageBuilderName}	aws:ResourceTag/ \${TagKey} (p. 121)
stack	arn:\${Partition}:appstream:\${Region}: \${Account}:stack/\${StackName}	aws:ResourceTag/ \${TagKey} (p. 121)
app-block	arn:\${Partition}:appstream:\${Region}: \${Account}:app-block/\${AppBlockName}	aws:ResourceTag/ \${TagKey} (p. 121)
application	arn:\${Partition}:appstream:\${Region}: \${Account}:application/\${ApplicationName}	aws:ResourceTag/ \${TagKey} (p. 121)

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 [Available global condition 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 \(p. 122\)](#)
- [Resource types defined by AWS AppSync \(p. 126\)](#)
- [Condition keys for AWS AppSync \(p. 126\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 126)		
CreateApiCache	Grants permission to create an API cache in AppSync	Write			
CreateApiKey	Grants permission to create a unique key that you can distribute to clients who are executing your API	Write			
CreateDataSource	Grants permission to create a data source	Write			
CreateDomainName	Grants permission to create a custom domain name in AppSync	Write			
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 , aws:ServiceLinkedRoleArn , \${TagKey} (p. 126) , aws:TagKeys (p. 126)	
CreateResolver	Grants permission to create a resolver. A resolver converts incoming requests into a format that a data source can	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	understand, and converts the data source's responses into GraphQL				
CreateType	Grants permission to create a type	Write			
DeleteApiCache	Grants permission to delete an API cache in AppSync	Write			
DeleteApiKey	Grants permission to delete an API key	Write			
DeleteDataSource	Grants permission to delete a data source	Write			
DeleteDomainName	Grants permission to delete a custom domain name in AppSync	Write	domain* (p. 126)		
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* (p. 126)		aws:ResourceTag/\${TagKey} (p. 126)
DeleteResolver	Grants permission to delete a resolver	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* (p. 126)		
FlushApiCache	Grants permission to flush an API cache in AppSync	Write			
GetApiAssociation	Grants permission to read custom domain name - GraphQL API association details in AppSync	Read	domain* (p. 126)		
GetApiCache	Grants permission to read information about an API cache in AppSync	Read			
GetDataSource	Grants permission to retrieve a data source	Read			
GetDomainName	Grants permission to read information about a custom domain name in AppSync	Read	domain* (p. 126)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetFunction	Grants permission to retrieve a function	Read			
GetGraphqlApi	Grants permission to retrieve a GraphQL API	Read	graphqlapi* (p. 126)		
				aws:ResourceTag/\${TagKey} (p. 126)	
GetIntrospectionSchema	Grants permission to retrieve the introspection schema for a GraphQL API	Read			
GetResolver	Grants permission to retrieve a resolver	Read			
GetSchemaCreationStatus	Grants permission to retrieve the current status of a schema creation operation	Read			
GetType	Grants permission to retrieve a type	Read			
GraphQL	Grants permission to send a GraphQL query to a GraphQL API	Write	field* (p. 126)		
			graphqlapi* (p. 126)		
ListApiKeys	Grants permission to list the API keys for a given API	List			
ListDataSources	Grants permission to list the data sources for a given API	List			
ListDomainNames	Grants permission to enumerate custom domain names in AppSync	List			
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			
ListTagsForResource	Grants permission to list the tags for a resource	Read	graphqlapi (p. 126)		
				aws:ResourceTag/\${TagKey} (p. 126)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTypes	Grants permission to list the types for a given API	List			
SetWebACL	Grants permission to set a web ACL	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			
TagResource	Grants permission to tag a resource	Tagging	graphqlapi (p. 126)		
				aws:RequestTag/\${TagKey} (p. 126)	
				aws:ResourceTag/\${TagKey} (p. 126)	
				aws:TagKeys (p. 126)	
UntagResource	Grants permission to untag a resource	Tagging	graphqlapi (p. 126)		
				aws:TagKeys (p. 126)	
UpdateApiCache	Grants permission to update an API cache in AppSync	Write			
UpdateApiKey	Grants permission to update an API key for a given API	Write			
UpdateDataSource	Grants permission to update a data source	Write			
UpdateDomainName	Grants permission to update a custom domain name in AppSync	Write	domain* (p. 126)		
UpdateFunction	Grants permission to update an existing function	Write			
UpdateGraphQLAPI	Grants permission to update a GraphQL API	Write	graphqlapi* (p. 126)		iam>CreateServiceLinkedRole (p. 126)
				aws:ResourceTag/\${TagKey} (p. 126)	
UpdateResolver	Grants permission to update a resolver	Write			
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 \(p. 122\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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}	
graphqlapi	arn:\${Partition}:appsync:\${Region}: \${Account}:apis/\${GraphQLAPIId}	aws:ResourceTag/\${TagKey} (p. 126)
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}	

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 [Available global condition 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 presence of tag keys in the request	String

Actions, resources, and condition keys for AWS Artifact

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

References:

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

Topics

- [Actions defined by AWS Artifact \(p. 127\)](#)
- [Resource types defined by AWS Artifact \(p. 128\)](#)
- [Condition keys for AWS Artifact \(p. 128\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 128)		
DownloadAgreement	Grants permission to download an AWS agreement that has not yet been accepted or a customer agreement that has been accepted by the customer account.	Read	agreement (p. 128)		
			customer-agreement (p. 128)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Get	Grants permission to download an AWS compliance report package.	Read	report-package* (p. 128)		
TerminateAgreement	Grants permission to terminate a customer agreement that was previously accepted by the customer account.	Write	customer-agreement* (p. 128)		

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 \(p. 127\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
report-package	arn:\${Partition}:artifact:::report-package/*	
customer-agreement	arn:\${Partition}:artifact:::\${Account}:customer-agreement/*	
agreement	arn:\${Partition}:artifact:::agreement/*	

Condition keys for AWS Artifact

Artifact 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 [Available keys for conditions](#).

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 \(p. 129\)](#)

- [Resource types defined by Amazon Athena \(p. 132\)](#)
- [Condition keys for Amazon Athena \(p. 132\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 132)		
BatchGetQueryExecution	Grants permission to get information about one or more query executions	Read	workgroup* (p. 132)		
CreateDataCatalog	Grants permission to create a <code>datacatalog</code>	Write	datacatalog* (p. 132)		
				aws:RequestTag/\${TagKey} (p. 132)	
CreateNamedQuery	Grants permission to create a <code>named query</code>	Write	workgroup* (p. 132)		
				aws:TagKeys (p. 132)	
CreatePreparedStatement	Grants permission to create a <code>prepared statement</code>	Write	workgroup* (p. 132)		
CreateWorkGroup	Grants permission to create a <code>workgroup</code>	Write	workgroup* (p. 132)		
				aws:RequestTag/\${TagKey} (p. 132)	
DeleteDataCatalog	Grants permission to delete a <code>datacatalog</code>	Write	datacatalog* (p. 132)		
				aws:TagKeys (p. 132)	
DeleteNamedQuery	Grants permission to delete a <code>named query</code> specified	Write	workgroup* (p. 132)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeletePreparedStatement	Grants permission to delete a prepared statement specified	Write	workgroup* (p. 132)		
DeleteWorkGroup	Grants permission to delete a workgroup	Write	workgroup* (p. 132)		
GetDataCatalog	Grants permission to get a datacatalog	Read	datacatalog* (p. 132)		
GetDatabase	Grants permission to get a database for a given datacatalog	Read	datacatalog* (p. 132)		
GetNamedQuery	Grants permission to get information about the specified named query	Read	workgroup* (p. 132)		
GetPreparedStatement	Grants permission to get information about the specified prepared statement	Read	workgroup* (p. 132)		
GetQueryExecution	Grants permission to get information about the specified query execution	Read	workgroup* (p. 132)		
GetQueryResults	Grants permission to get the query results	Read	workgroup* (p. 132)		
GetQueryResultsStream	Grants permission to get the query results stream	Read	workgroup* (p. 132)		
GetTableMetadata	Grants permission to get a metadata about a table for a given datacatalog	Read	datacatalog* (p. 132)		
GetWorkGroup	Grants permission to get a workgroup	Read	workgroup* (p. 132)		
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* (p. 132)		
ListEngineVersions	Grants permission to return a list of athena engine versions for the specified AWS account	Read			
ListNamedQueries	Grants permission to return a list of named queries in Amazon Athena for the specified AWS account	List	workgroup* (p. 132)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPreparedStatements	Grants permission to return a list of prepared statements for the specified workgroup	List	workgroup* (p. 132)		
ListQueryExecutions	Grants permission to return a list of query executions for the specified AWS account	Read	workgroup* (p. 132)		
ListTableMetadata	Grants permission to return a list of table metadata in a database for a given datacatalog	Read	datacatalog* (p. 132)		
ListTagsForResource	Grants permission to return a list of tags for a resource	Read	datacatalog* (p. 132)		
ListWorkGroups	Grants permission to return a list of workgroups for the specified AWS account		workgroup* (p. 132)		
StartQueryExecution	Grants permission to start a query execution using an SQL query provided as a string	Write	workgroup* (p. 132)		
StopQueryExecution	Grants permission to stop the specified query execution	Write	workgroup* (p. 132)		
TagResource	Grants permission to add a tag to a resource	Tagging	datacatalog* (p. 132)		
workgroup* (p. 132)					
	aws:RequestTag/ \${TagKey} (p. 132)				
	aws:TagKeys (p. 132)				
UntagResource	Grants permission to remove a tag from a resource	Tagging	datacatalog* (p. 132)		
workgroup* (p. 132)					
	aws:TagKeys (p. 132)				
UpdateDataCatalog	Grants permission to update a datacatalog	Write	datacatalog* (p. 132)		
UpdateNamedQuery	Grants permission to update a named query specified	Write	workgroup* (p. 132)		
UpdatePreparedStatement	Grants permission to update a prepared statement	Write	workgroup* (p. 132)		
UpdateWorkGroup	Grants permission to update a workgroup	Write	workgroup* (p. 132)		

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 \(p. 129\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
datacatalog	<code>arn:\${Partition}:athena:\${Region}:\${Account}:datacatalog/\${DataCatalogName}</code>	aws:ResourceTag/\${TagKey} (p. 132)
workgroup	<code>arn:\${Partition}:athena:\${Region}:\${Account}:workgroup/\${WorkGroupName}</code>	aws:ResourceTag/\${TagKey} (p. 132)

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 [Available global condition 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 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 \(p. 133\)](#)
- [Resource types defined by AWS Audit Manager \(p. 138\)](#)
- [Condition keys for AWS Audit Manager \(p. 138\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateAssessmentEvidenceFolderWithAn assessment report in AWS Audit Manager	Grants permission to associate a <code>list of evidence</code> to an <code>assessment</code> report in AWS Audit Manager	Write	assessment* (p. 138)		
BatchAssociateAssessments	Grants permission to associate a <code>list of evidence</code> to an <code>assessment</code> report in AWS Audit Manager	Write	assessment* (p. 138)		
BatchCreateDelegations	Grants permission to create <code>delegations</code> for an <code>assessment</code> in AWS Audit Manager	Write	assessment* (p. 138)		
BatchDeleteDelegations	Grants permission to delete <code>delegations</code> for an <code>assessment</code> in AWS Audit Manager	Write	assessment* (p. 138)		
BatchDisassociateEvidence	Grants permission to <code>disassociate</code> a <code>list of evidence</code> from an <code>assessment</code> report in AWS Audit Manager	Write	assessment* (p. 138)		
BatchImportEvidence	Grants permission to import a <code>list of evidence</code> to an <code>assessment</code> control in AWS Audit Manager	Write	assessmentControlSet* (p. 138)		
CreateAssessment	Grants permission to create an <code>assessment</code> to be used with AWS Audit Manager	Write		<code>aws:RequestTag/\${TagKey}</code> (p. 139) <code>aws:TagKeys</code> (p. 139)	
CreateAssessmentFramework	Grants permission to create a <code>framework</code> for use in AWS Audit Manager	Write		<code>aws:RequestTag/\${TagKey}</code> (p. 139) <code>aws:TagKeys</code> (p. 139)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAssessment	Grants permission to create an assessment report in AWS Audit Manager	Write	assessment* (p. 138)		
CreateControl	Grants permission to create a control to be used in AWS Audit Manager	Write		aws:RequestTag/\${TagKey} (p. 139)	
DeleteAssessment	Grants permission to delete an assessment in AWS Audit Manager	Write	assessment* (p. 138)		
			aws:RequestTag/\${TagKey} (p. 139)		
DeleteAssessmentFramework	Grants permission to delete an assessment framework in AWS Audit Manager	Write	assessmentFramework* (p. 138)		
			aws:RequestTag/\${TagKey} (p. 139)		
DeleteAssessmentFrameworkShareRequest	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* (p. 138)		
DeleteControl	Grants permission to delete a control in AWS Audit Manager	Write	control* (p. 138)		
			aws:RequestTag/\${TagKey} (p. 139)		
DeregisterAccount	Grants permission to deregister an account in AWS Audit Manager	Write			
DeregisterOrganizationDelegatedAdministrator	Grants permission to deregister the delegated administrator account for AWS Audit Manager	Write			
DisassociateAssessmentEvidenceFolder	Grants permission to disassociate an evidence folder from an assessment report in AWS Audit Manager	Write	assessment* (p. 138)		
GetAccountStatus	Grants permission to get the status of an account in AWS Audit Manager	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAssessment	Grants permission to get an assessment created in AWS Audit Manager	Read	assessment* (p. 138)		
GetAssessmentFramework	Grants permission to get an assessment framework in AWS Audit Manager	Read	assessmentFramework* (p. 138)		
GetAssessmentReportUrl	Grants permission to get the URL for an assessment report in AWS Audit Manager	Read	assessment* (p. 138)		
GetChangeLogs	Grants permission to get changelogs for an assessment in AWS Audit Manager	Read	assessment* (p. 138)		
GetControl	Grants permission to get a control in AWS Audit Manager	Read	control* (p. 138)		
GetDelegations	Grants permission to get all delegations in AWS Audit Manager	List			
GetEvidence	Grants permission to get evidence from AWS Audit Manager	Read	assessmentControlSet* (p. 138)		
GetEvidenceByEvidenceId	Grants permission to get all the evidence from an evidence folder in AWS Audit Manager	Read	assessmentControlSet* (p. 138)		
GetEvidenceFolder	Grants permission to get the evidence folder from AWS Audit Manager	Read	assessmentControlSet* (p. 138)		
GetEvidenceFoldersFromAssessment	Grants permission to get the evidence folders from an assessment in AWS Audit Manager	Read	assessment* (p. 138)		
GetEvidenceFoldersFromControl	Grants permission to get the evidence folders from an assessment control in AWS Audit Manager	Read	assessmentControlSet* (p. 138)		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetOrganizationDelegatedAdministrator	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			
ListAssessmentControlsInActiveAssessments	Grants permission to list controls in a specific control domain and active assessment	List			
ListAssessmentFrameworkShareRequests	Grants permission to list all sent share requests for custom frameworks in AWS Audit Manager	List			
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			
ListControlDomainAnalytics	Grants permission to list analytics data for control domains across all active assessments	List			
ListControlDomainAnalyticsForControlDomain	Grants permission to list analytics data for control domains in a specific active assessment	List			
ListControlInsights	Grants permission to list insights 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 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 (p. 138)		
			control (p. 138)		
RegisterAccount	Grants permission to register an account in AWS Audit Manager	Write			
RegisterOrganizationAccount	Grants permission to register an account within the organization as the delegated administrator for AWS Audit Manager	Write			
StartAssessment	CreateAssessmentRequest	Write	assessmentFramework* (p. 138)		
TagResource	Grants permission to tag an AWS Audit Manager resource	Tagging	assessment (p. 138)		
			control (p. 138)		
				aws:TagKeys (p. 139)	
				aws:RequestTag/ \${TagKey} (p. 139)	
UntagResource	Grants permission to untag an AWS Audit Manager resource	Tagging	assessment (p. 138)		
			control (p. 138)		
				aws:TagKeys (p. 139)	
UpdateAssessment	Grants permission to update an assessment in AWS Audit Manager	Write	assessment* (p. 138)		
UpdateAssessmentControl	Grants permission to update an assessment control in AWS Audit Manager	Write	assessmentControlSet* (p. 138)		
UpdateAssessmentControlSet	Grants permission to update the status of an assessment control set in AWS Audit Manager	Write	assessmentControlSet* (p. 138)		
UpdateAssessmentFramework	Grants permission to update an assessment framework in AWS Audit Manager	Write	assessmentFramework* (p. 138)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAssessment	Grants permission to update a share request for a custom framework in AWS Audit Manager	Write			
UpdateAssessmentStatus	Grants permission to update the status of an assessment in AWS Audit Manager	Write	assessment* (p. 138)		
UpdateControl	Grants permission to update a control in AWS Audit Manager	Write	control* (p. 138)		
UpdateSettings	Grants permission to update settings in AWS Audit Manager	Write			
ValidateAssessment	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 \(p. 133\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
assessment	<code>arn:\${Partition}:auditmanager:\${Region}: \${Account}:assessment/\${AssessmentId}</code>	
assessmentFramework	<code>arn:\${Partition}:auditmanager:\${Region}: \${Account}:assessmentFramework/ \${AssessmentFrameworkId}</code>	
assessmentControlSet	<code>arn:\${Partition}:auditmanager:\${Region}: \${Account}:assessment/\${AssessmentId}/ ControlSet/\${ControlSetId}</code>	
control	<code>arn:\${Partition}:auditmanager:\${Region}: \${Account}:control/\${ControlId}</code>	aws:ResourceTag/ \${TagKey} (p. 139)

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 [Available global condition keys](#).

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

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 \(p. 139\)](#)
- [Resource types defined by AWS Auto Scaling \(p. 140\)](#)
- [Condition keys for AWS Auto Scaling \(p. 140\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteScalingPlan	Deletes the specified scaling plan.	Write			
DescribeScalingPlans	Describes the scalable resources in the specified scaling plan.	Read			
DescribeScalingPlans	Describes the specified scaling plans or all of your scaling plans.	Read			
GetScalingPlanForecastData	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 [Available keys for conditions](#).

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 \(p. 140\)](#)
- [Resource types defined by AWS Backup \(p. 146\)](#)
- [Condition keys for AWS Backup \(p. 147\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CopyFromBackupVault [permission only]	Grants permission to copy from a backup vault	Write		backup:CopyTargets (p. 147) backup:CopyTargetOrgPaths (p. 147)	
CopyIntoBackupVault [permission only]	Grants permission to copy into a backup vault	Write		aws:RequestTag/\${TagKey} (p. 147)	
CreateBackupPlan	Grants permission to create a new backup plan	Write	backupPlan* (p. 146)		
				aws:RequestTag/\${TagKey} (p. 147) aws:TagKeys (p. 147)	
CreateBackupSelection	Grants permission to create a new resource assignment in a backup plan	Write	backupPlan* (p. 146)	iam:PassRole	
CreateBackupVault	Grants permission to create a new backup vault	Write	backupVault* (p. 146)		
				aws:RequestTag/\${TagKey} (p. 147) aws:TagKeys (p. 147)	
CreateFramework	Grants permission to create a new framework	Write	framework* (p. 146)		
				aws:RequestTag/\${TagKey} (p. 147) aws:TagKeys (p. 147)	
CreateReportPlan	Grants permission to create a new report plan	Write	reportPlan* (p. 146)		
				aws:RequestTag/\${TagKey} (p. 147) aws:TagKeys (p. 147) backup:FrameworkArns (p. 147)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteBackupPlan	Grants permission to delete a backup plan	Write	backupPlan* (p. 146)		
DeleteBackupSelection	Grants permission to delete a resource assignment from a backup plan	Write	backupPlan* (p. 146)		
DeleteBackupVault	Grants permission to delete a backup vault	Write	backupVault* (p. 146)		
DeleteBackupVaultAccessPolicy	Grants permission to delete a backup vault access policy	Permissions management	backupVault* (p. 146)		
DeleteBackupVaultLockConfiguration	Grants permission to remove the lock configuration from a backup vault	Write	backupVault* (p. 146)		
DeleteBackupVaultNotification	Grants permission to remove the notifications from a backup vault	Write	backupVault* (p. 146)		
DeleteFramework	Grants permission to delete a framework	Write	framework* (p. 146)		
DeleteRecoveryPoint	Grants permission to delete a recovery point from a backup vault	Write	recoveryPoint* (p. 146)		
DeleteReportPlan	Grants permission to delete a report plan	Write	reportPlan* (p. 146)		
DescribeBackupJob	Grants permission to describe a backup job	Read			
DescribeBackupVault	Grants permission to describe a new backup vault with the specified name	Read	backupVault* (p. 146)		
DescribeCopyJob	Grants permission to describe a copy job	Read			
DescribeFramework	Grants permission to describe a framework with the specified name	Read	framework* (p. 146)		
DescribeGlobalSettings	Grants permission to describe global settings	Read			
DescribeProtectedResource	Grants permission to describe a protected resource	Read			
DescribeRecoveryPoint	Grants permission to describe a recovery point	Read	recoveryPoint* (p. 146)		
DescribeRegionSettings	Grants permission to describe region settings	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeReportJob	Grants permission to describe a report job	Read			
DescribeReportPlan	Grants permission to describe a report plan with the specified name	Read	reportPlan* (p. 146)		
DescribeRestoreJob	Grants permission to describe a restore job	Read			
DisassociateRecoveryPoint	Grants permission to disassociate a recovery point from a backup vault	Write	recoveryPoint* (p. 146)		
ExportBackupPlan	Grants permission to export a backup plan as a JSON	Read			
GetBackupPlan	Grants permission to get a backup plan	Read	backupPlan* (p. 146)		
GetBackupPlanFromTemplate	Grants permission to transform a JSON template to a backup plan	Read			
GetBackupPlanFromTemplate	Grants permission to transform an AWS Backup template to a backup plan	Read			
GetBackupSelection	Grants permission to get a backup plan resource assignment	Read	backupPlan* (p. 146)		
GetBackupVaultAccessPolicy	Grants permission to get backup vault access policy	Read	backupVault* (p. 146)		
GetBackupVaultNotifications	Grants permission to get backup vault notifications	Read	backupVault* (p. 146)		
GetRecoveryPointMetadata	Grants permission to get recovery point restore metadata	Read	recoveryPoint* (p. 146)		
GetSupportedResourceTypes	Grants permission to get supported resource types	Read			
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* (p. 146)		
ListBackupPlans	Grants permission to list backup plans	List			

Service Authorization Reference
Service Authorization Reference
AWS Backup

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListBackupSelections	Grants permission to list resource assignments for a specific backup plan	List	backupPlan* (p. 146)		
ListBackupVaults	Grants permission to list backup vaults	List			
ListCopyJobs	Grants permission to list copy jobs	List			
ListFrameworks	Grants permission to list frameworks	List			
ListProtectedResources	Grants permission to list protected resources by AWS Backup	List			
ListRecoveryPoints	Grants permission to list recovery points inside a backup vault	List	backupVault* (p. 146)		
ListRecoveryPointDetails	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			
ListRestoreJobs	Grants permission to lists restore jobs	List			
ListTags	Grants permission to list tags for a resource	Read	backupPlan (p. 146)		
			backupVault (p. 146)		
			framework (p. 146)		
			recoveryPoint (p. 146)		
			reportPlan (p. 146)		
PutBackupVaultAccessPolicy	Grants permission to add an access policy to the backup vault	Permissions management	backupVault* (p. 146)		
PutBackupVaultLockConfiguration	Grants permission to add a lock configuration to the backup vault	Write	backupVault* (p. 146)		
PutBackupVaultNotificationTopic	Grants permission to add an SNS topic to the backup vault	Write	backupVault* (p. 146)		
StartBackupJob	Grants permission to start a new backup job	Write	backupVault* (p. 146)	iam:PassRole	

Service Authorization Reference
Service Authorization Reference
AWS Backup

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 147) aws:TagKeys (p. 147)	
StartCopyJob	Grants permission to copy a backup from a source backup vault to a destination backup vault	Write	recoveryPoint* (p. 146)	iam:PassRole	
StartReportJob	Grants permission to start a new report job	Write	reportPlan* (p. 146)		
StartRestoreJob	Grants permission to start a new restore job	Write	recoveryPoint* (p. 146)	iam:PassRole	
StopBackupJob	Grants permission to stop a backup job	Write			
TagResource	Grants permission to tag a resource	Tagging	backupPlan (p. 146)		
			backupVault (p. 146)		
			framework (p. 146)		
			recoveryPoint (p. 146)		
			reportPlan (p. 146)		
			aws:RequestTag/ \${TagKey} (p. 147)		
			aws:TagKeys (p. 147)		
UntagResource	Grants permission to untag a resource	Tagging	backupPlan (p. 146)		
			backupVault (p. 146)		
			framework (p. 146)		
			recoveryPoint (p. 146)		
			reportPlan (p. 146)		
			aws:TagKeys (p. 147)		
UpdateBackupPlan	Grants permission to update a backup plan	Write	backupPlan* (p. 146)		
			aws:RequestTag/ \${TagKey} (p. 147)		
			aws:TagKeys (p. 147)		
UpdateFramework	Grants permission to update a framework	Write	framework* (p. 146)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 147) aws:TagKeys (p. 147)	
UpdateGlobalSettings	Grants permission to update the current global settings for the AWS Account	Write			
UpdateRecoveryPointLifecycle	Grants permission to update the lifecycle of the recovery point	Write	recoveryPoint* (p. 146)		
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* (p. 146)		backup:FrameworkArns (p. 147)

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 \(p. 140\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 147)
backupPlan	arn:\${Partition}:backup:\${Region}: \${Account}:backup-plan:\${BackupPlanId}	aws:ResourceTag/ \${TagKey} (p. 147)
recoveryPoint	arn:\${Partition}: \${Vendor}: \${Region}:*: \${ResourceType}: \${RecoveryPointId}	aws:ResourceTag/ \${TagKey} (p. 147)
framework	arn:\${Partition}:backup:\${Region}: \${Account}:framework:\${FrameworkName}- \${FrameworkId}	aws:ResourceTag/ \${TagKey} (p. 147)
reportPlan	arn:\${Partition}:backup:\${Region}: \${Account}:report-plan:\${ReportPlanName}- \${ReportPlanId}	aws:ResourceTag/ \${TagKey} (p. 147)

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters access by the allowed set of values for each of the tags	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters access by the tags associated with the resource	String
<code>aws:TagKeys</code>	Filters access by the presence of mandatory tags in the request	ArrayOfString
<code>backup:CopyTargetOrgPaths</code>	Filters access by the organization unit	ArrayOfString
<code>backup:CopyTargets</code>	Filters access by the ARN of an backup vault	ArrayOfARN
<code>backup:FrameworkArns</code>	Filters access by the Framework ARNs	ArrayOfARN

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 \(p. 147\)](#)
- [Resource types defined by AWS Backup Gateway \(p. 149\)](#)
- [Condition keys for AWS Backup Gateway \(p. 150\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateGateway	Grants permission to <code>AssociateGatewayToServer</code>	Write	gateway* (p. 150)		
			hypervisor* (p. 150)		
Backup	Grants permission to <code>Backup</code>	Write	virtualmachine* (p. 150)		
			aws:RequestTag/ {\$TagKey} (p. 150)		
			aws:TagKeys (p. 150)		
CreateGateway	Grants permission to <code>CreateGateway</code>	Write		aws:RequestTag/ {\$TagKey} (p. 150)	
				aws:TagKeys (p. 150)	
DeleteGateway	Grants permission to <code>DeleteGateway</code>	Write	gateway* (p. 150)		
DeleteHypervisor	Grants permission to <code>DeleteHypervisor</code>	Write	hypervisor* (p. 150)		
DisassociateGatewayFromServer	Grants permission to <code>DisassociateGatewayFromServer</code>	Write	gateway* (p. 150)		
GetGateway	Grants permission to <code>GetGateway</code>	Read	gateway* (p. 150)		
ImportHypervisorConfiguration	Grants permission to <code>ImportHypervisorConfiguration</code>	Write		aws:RequestTag/ {\$TagKey} (p. 150)	
				aws:TagKeys (p. 150)	
ListGateways	Grants permission to <code>ListGateways</code>	Read			
ListHypervisors	Grants permission to <code>ListHypervisors</code>	Read			
ListTagsForResource	Grants permission to <code>ListTagsForResource</code>	Read	gateway (p. 150)		
			hypervisor (p. 150)		
			virtualmachine (p. 150)		
			aws:RequestTag/ {\$TagKey} (p. 150)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys (p. 150)	
ListVirtualMachines	Grants permission to ListVirtualMachines	Read			
PutMaintenanceStartTime	Grants permission to PutMaintenanceStartTime	Write	gateway* (p. 150)		
Restore	Grants permission to Restore	Write	hypervisor* (p. 150)		
				aws:RequestTag/ \${TagKey} (p. 150)	
				aws:TagKeys (p. 150)	
TagResource	Grants permission to TagResource	Tagging	gateway (p. 150)		
			hypervisor (p. 150)		
			virtualmachine (p. 150)		
				aws:RequestTag/ \${TagKey} (p. 150)	
				aws:TagKeys (p. 150)	
TestHypervisorConfiguration	Grants permission to TestHypervisorConfiguration	Write	gateway* (p. 150)		
UntagResource	Grants permission to UntagResource	Tagging	gateway (p. 150)		
			hypervisor (p. 150)		
			virtualmachine (p. 150)		
				aws:RequestTag/ \${TagKey} (p. 150)	
				aws:TagKeys (p. 150)	
UpdateGatewayInformation	Grants permission to UpdateGatewayInformation	Write	gateway* (p. 150)		
UpdateGatewaySoftwareNow	Grants permission to UpdateGatewaySoftwareNow	Write	gateway* (p. 150)		
UpdateHypervisor	Grants permission to UpdateHypervisor	Write	gateway* (p. 150)		

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 \(p. 147\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
gateway	arn:\${Partition}:backup-gateway::\${Account}:gateway/\${GatewayId}	aws:ResourceTag/\${TagKey} (p. 150)
hypervisor	arn:\${Partition}:backup-gateway::\${Account}:hypervisor/\${HypervisorId}	aws:ResourceTag/\${TagKey} (p. 150)
virtualmachine	arn:\${Partition}:backup-gateway::\${Account}:vm/\${VirtualmachineId}	aws:ResourceTag/\${TagKey} (p. 150)

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 [Available global condition 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 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 \(p. 151\)](#)
- [Resource types defined by AWS Backup storage \(p. 151\)](#)
- [Condition keys for AWS Backup storage \(p. 151\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
MountCapsule [permission only]	Associates a KMS key to a backup vault	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 [Available keys for conditions](#).

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 \(p. 152\)](#)
- [Resource types defined by AWS Batch \(p. 155\)](#)
- [Condition keys for AWS Batch \(p. 156\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 156)		
CreateComputeEnvironment	Grants permission to create an AWS Batch compute environment in your account	Write	compute-environment* (p. 155)		
				aws:RequestTag/\${TagKey} (p. 156)	aws:TagKeys (p. 156)
CreateJobQueue	Grants permission to create an AWS Batch job queue in your account	Write	compute-environment* (p. 155)		
			job-queue* (p. 155)		
			scheduling-policy (p. 156)		
				aws:RequestTag/\${TagKey} (p. 156)	aws:TagKeys (p. 156)
CreateSchedulingPolicy	Grants permission to create an AWS Batch scheduling policy in your account	Write	scheduling-policy* (p. 156)		
				aws:RequestTag/\${TagKey} (p. 156)	aws:TagKeys (p. 156)
DeleteComputeEnvironment	Grants permission to delete an AWS Batch compute environment in your account	Write	compute-environment* (p. 155)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteJobQueue	Grants permission to delete an AWS Batch job queue in your account	Write	job-queue* (p. 155)		
DeleteSchedulingPolicy	Grants permission to delete an AWS Batch scheduling policy in your account	Write	scheduling-policy* (p. 156)		
DeregisterJobDefinition	Grants permission to deregister an AWS Batch job definition in your account	Write	job-definition* (p. 156)		
DescribeComputeEnvironments	Grants permission to describe one or more AWS Batch compute environments in your account	Read			
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			
DescribeSchedulingPolicies	Grants permission to describe one or more AWS Batch scheduling policies in your account	Read			
ListJobs	Grants permission to list jobs for a specified AWS Batch job queue in your account	List			
ListSchedulingPolicies	Grants permission to list AWS Batch scheduling policies in your account	Read			
ListTagsForResource	Grants permission to list tags for an AWS Batch resource in your account	Read	compute-environment (p. 155)		
			job (p. 156)		
			job-definition (p. 156)		
			job-queue (p. 155)		
			scheduling-policy (p. 156)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterJobDefinition	Grants permission to register an AWS Batch job definition in your account	Write	job-definition* (p. 156) batch:User (p. 156) batch:Privileged (p. 156) batch:Image (p. 156) batch:LogDriver (p. 156) batch:AWSLogsGroup (p. 156) batch:AWSLogsRegion (p. 156) batch:AWSLogsStreamPrefix (p. 156) batch:AWSLogsCreateGroup (p. 156) aws:RequestTag/ {\$TagKey} (p. 156) aws:TagKeys (p. 156)		
SubmitJob	Grants permission to submit an AWS Batch job from a job definition in your account	Write	job-definition* (p. 156) job-queue* (p. 155)		
TagResource	Grants permission to tag an AWS Batch resource in your account	Tagging	compute-environment (p. 155) job (p. 156) job-definition (p. 156) job-queue (p. 155) scheduling-policy (p. 156) aws:RequestTag/ {\$TagKey} (p. 156) aws:TagKeys (p. 156)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TerminateJob	Grants permission to terminate a job in an AWS Batch job queue in your account	Write	job* (p. 156)		
UntagResource	Grants permission to untag an AWS Batch resource in your account	Tagging	compute-environment (p. 155)		
			job (p. 156)		
			job-definition (p. 156)		
			job-queue (p. 155)		
			scheduling-policy (p. 156)		
				aws:TagKeys (p. 156)	
UpdateComputeEnvironment	Grants permission to update an AWS Batch compute environment in your account	Write	compute-environment* (p. 155)		
UpdateJobQueue	Grants permission to update an AWS Batch job queue in your account	Write	job-queue* (p. 155)		
			compute-environment (p. 155)		
			scheduling-policy (p. 156)		
UpdateSchedulingPolicy	Grants permission to update an AWS Batch scheduling policy in your account	Write	scheduling-policy* (p. 156)		

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 \(p. 152\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 156)
job-queue	arn:\${Partition}:batch:\${Region}:\${Account}:job-queue/\${JobQueueName}	aws:ResourceTag/\${TagKey} (p. 156)

Resource types	ARN	Condition keys
job-definition	arn:\${Partition}:batch:\${Region}: \${Account}:job-definition/ \${JobDefinitionName}:\${Revision}	aws:ResourceTag/ \${TagKey} (p. 156)
job	arn:\${Partition}:batch:\${Region}: \${Account}:job/\${JobId}	aws:ResourceTag/ \${TagKey} (p. 156)
scheduling-policy	arn:\${Partition}:batch:\${Region}: \${Account}:scheduling-policy/ \${SchedulingPolicyName}	aws:ResourceTag/ \${TagKey} (p. 156)

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 [Available global condition 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:AWSLogsCreateWhether	Filters access by the specified logging driver to determine whether awslogs group will be created for the logs	Bool
batch:AWSLogsGrouplocated	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:Image	Filters access by on the image used to start a container	String
batch:LogDriver	Filters access by the log driver used for the container	String
batch:Privileged	Filters access by the specified privileged parameter value that determines whether the container is given elevated privileges on the host container instance (similar to the root user)	Bool
batch:ShareIdentifier	Filters access by the shareIdentifier used inside submit job	String
batch:User	Filters access by user name or numeric uid used inside the container	String

Actions, resources, and condition keys for AWS Billing and Cost Management

AWS Billing and Cost Management (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 and Cost Management \(p. 157\)](#)
- [Resource types defined by AWS Billing and Cost Management \(p. 158\)](#)
- [Condition keys for AWS Billing and Cost Management \(p. 158\)](#)

Actions defined by AWS Billing and Cost 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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyAccount	Allow or deny IAM users permission to modify Account Settings.	Write			
ModifyBilling	Allow or deny IAM users permission to modify billing settings.	Write			
ModifyPaymentMethod	Allow or deny IAM users permission to modify payment methods.	Write			
ViewAccount	Allow or deny IAM users permission to view account settings.	Read			

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

Resource types defined by AWS Billing and Cost Management

AWS Billing and Cost Management 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, specify “`Resource`”: “`**`” in your policy.

Condition keys for AWS Billing and Cost Management

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 [Available keys for conditions](#).

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 \(p. 158\)](#)
- [Resource types defined by AWS Billing Conductor \(p. 161\)](#)
- [Condition keys for AWS Billing Conductor \(p. 161\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateAccount	Grants permission to associate between one and 30 accounts to a billing group	Write	billinggroup* (p. 161)		
AssociatePricingRule	Grants permission to associate pricing rules	Write	pricingplan* (p. 161) pricingrule* (p. 161)		
BatchAssociateResourcesToItem	Grants permission to batch associate resources to a percentage custom line item	Write	customlineitem* (p. 161)		
BatchDisassociateResourcesFromItem	Grants permission to batch disassociate resources from a percentage custom line item	Write	customlineitem* (p. 161)		
CreateBillingGroup	Grants permission to create a billing group	Write	pricingplan* (p. 161) aws:TagKeys (p. 162) aws:RequestTag/\${TagKey} (p. 162)		
CreateCustomLineItem	Grants permission to create a custom line item	Write		aws:TagKeys (p. 162) aws:RequestTag/\${TagKey} (p. 162)	
CreatePricingPlan	Grants permission to create a pricing plan	Write		aws:TagKeys (p. 162) aws:RequestTag/\${TagKey} (p. 162)	
CreatePricingRule	Grants permission to create a pricing rule	Write		aws:TagKeys (p. 162) aws:RequestTag/\${TagKey} (p. 162)	
DeleteBillingGroup	Grants permission to delete a billing group	Write	billinggroup* (p. 161)		
DeleteCustomLineItem	Grants permission to delete a custom line item	Write	customlineitem* (p. 161)		
DeletePricingPlan	Grants permission to delete a pricing plan	Write	pricingplan* (p. 161)		

Service Authorization Reference
Service Authorization Reference
AWS Billing Conductor

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeletePricingRule	Grants permission to delete a pricing rule	Write	pricingrule* (p. 161)		
DisassociateAccount	Grants permission to detach between one and 30 accounts from a billing group	Write	billinggroup* (p. 161)		
DisassociatePricingRule	Grants permission to disassociate pricing rules	Write	pricingplan* (p. 161)		
			pricingrule* (p. 161)		
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			
ListBillingGroups	Grants permission to view the details of billing groups	Read			
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	pricingplan* (p. 161)		
			pricingrule* (p. 161)		
ListPricingRules	Grants permission to view pricing rules details	Read			
ListPricingRulesAssociatedWithPricingPlan	Grants permission to list pricing rules associated with a pricing plan	List	pricingplan* (p. 161)		
			pricingrule* (p. 161)		
ListResourcesAssociatedToACustomLineItem	Grants permission to list resources associated to a percentage custom line item	List	customlineitem* (p. 161)		
ListTagsForResource	Grants permission to list tags of a resource	Read		aws:TagKeys (p. 162) aws:RequestTag/\${TagKey} (p. 162)	
TagResource	Grants permission to tag a resource	Tagging		aws:TagKeys (p. 162) aws:RequestTag/\${TagKey} (p. 162)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagResource	Grants permission to untag a resource	Tagging		aws:TagKeys (p. 162) aws:RequestTag/\${TagKey} (p. 162)	
UpdateBillingGroup	Grants permission to update a billing group	Write	billinggroup* (p. 161)		
UpdateCustomLineItem	Grants permission to update a custom line item	Write	customlineitem* (p. 161)		
UpdatePricingPlan	Grants permission to update a pricing plan	Write	pricingplan* (p. 161)		
UpdatePricingRule	Grants permission to update a pricing rule	Write	pricingrule* (p. 161)		

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 \(p. 158\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 162)
pricingplan	arn:\${Partition}:billingconductor::\${Account}:pricingplan/\${PricingPlanId}	aws:ResourceTag/\${TagKey} (p. 162)
pricingrule	arn:\${Partition}:billingconductor::\${Account}:pricingrule/\${PricingRuleId}	aws:ResourceTag/\${TagKey} (p. 162)
customlineitem	arn:\${Partition}:billingconductor::\${Account}:customlineitem/\${CustomLineItemId}	aws:ResourceTag/\${TagKey} (p. 162)

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 [Available global condition keys](#).

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

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 \(p. 162\)](#)
- [Resource types defined by Amazon Braket \(p. 164\)](#)
- [Condition keys for Amazon Braket \(p. 164\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
<code>CancelJob</code>	Grants permission to cancel a job	Write	job* (p. 164)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelQuantumTask	Grants permission to cancel a quantum task	Write	quantum-task* (p. 164)		
CreateJob	Grants permission to create a job	Write		aws:RequestTag/\${TagKey} (p. 164) aws:TagKeys (p. 164)	
CreateQuantumTask	Grants permission to create a quantum task	Write		aws:RequestTag/\${TagKey} (p. 164) aws:TagKeys (p. 164)	
GetDevice	Grants permission to retrieve information about the devices available in Amazon Braket	Read			
GetJob	Grants permission to retrieve jobs	Read	job* (p. 164)		
GetQuantumTask	Grants permission to retrieve quantum tasks	Read	quantum-task* (p. 164)		
ListTagsForResource	Grants permission to listing the tags that have been applied to the quantum task resource or the job	Read	job (p. 164) quantum-task (p. 164)		
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			
TagResource	Grants permission to add one or more tags to a quantum task	Tagging	quantum-task (p. 164)		
				aws:RequestTag/\${TagKey} (p. 164) aws:TagKeys (p. 164)	
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 (p. 164) quantum-task (p. 164)		
				aws:TagKeys (p. 164)	

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 \(p. 162\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
quantum-task	<code>arn:\${Partition}:braket:\${Region}:\${Account}:quantum-task/\${RandomId}</code>	aws:ResourceTag/\${TagKey} (p. 164)
job	<code>arn:\${Partition}:braket:\${Region}:\${Account}:job/\${JobName}</code>	aws:ResourceTag/\${TagKey} (p. 164)

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 [Available global condition 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 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 \(p. 165\)](#)
- [Resource types defined by AWS Budget Service \(p. 166\)](#)
- [Condition keys for AWS Budget Service \(p. 166\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 permissions to create and define a response that you can configure to execute once your budget has exceeded a specific budget threshold.	Write	budgetAction* (p. 166)		iam:PassRole
DeleteBudgetAction	Grants permissions to delete an action that is associated with a specific budget.	Write	budgetAction* (p. 166)		
DescribeBudgetAction	Grants permissions to retrieve the details of specific budget action associated with a budget.	Read	budgetAction* (p. 166)		
DescribeBudgetActionHistory	Grants permissions to retrieve a historical view of the budget actions statuses associated with a particular budget action. These status include statuses such as 'Standby', 'Pending' and 'Executed'.	Read	budgetAction* (p. 166)		
DescribeBudgetActions	Grants permissions to retrieve the details of all the budget actions associated with your account.	Read			
DescribeBudgetActionSummary	Grants permissions to retrieve the details of all the budget actions associated with a budget.	Read	budget* (p. 166)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ExecuteBudgetAction	Grants permissions to initiate a pending budget action as well as reverse a previously executed budget action.	Write	budgetAction* (p. 166)		
ModifyBudget	Grants permissions to modify budgets and budget details	Write	budget* (p. 166)		
UpdateBudgetAction	Grants permissions to update the details of a specific budget action associated with a budget.	Write	budgetAction* (p. 166)	iam:PassRole	
ViewBudget	Grants permissions to view budgets and budget details	Read	budget* (p. 166)		

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 \(p. 165\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
budget	<code>arn:\${Partition}:budgets::\${Account}:budget/\${BudgetName}</code>	
budgetAction	<code>arn:\${Partition}:budgets::\${Account}:budget/\${BudgetName}/action/\${ActionId}</code>	

Condition keys for AWS Budget Service

Budget 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 [Available keys for conditions](#).

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 \(p. 167\)](#)
- [Resource types defined by AWS BugBust \(p. 169\)](#)
- [Condition keys for AWS BugBust \(p. 170\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 (p. 170) aws:RequestTag/ \${TagKey} (p. 170)	CreateServiceLinkedRole
EvaluateProfiling [permission only]	Grants permission to evaluate checked-in profiling groups	Write	Event* (p. 169)	aws:ResourceTag/ \${TagKey} (p. 170)	
GetEvent [permission only]	Grants permission to view customer details about an event	Read	Event* (p. 169)	aws:ResourceTag/ \${TagKey} (p. 170)	
GetJoinEventStats [permission only]	Grants permission to view the status of a BugBust player's attempt to join a BugBust event	Read	Event* (p. 169)	aws:ResourceTag/ \${TagKey} (p. 170)	
JoinEvent [permission only]	Grants permission to join an event	Write	Event* (p. 169)	aws:ResourceTag/ \${TagKey} (p. 170)	
ListBugs [permission only]	Grants permission to view the bugs that were imported into an event for players to work on	Read	Event* (p. 169)		codeguru-reviewer:DescribeCodeReview codeguru-reviewer>ListRecommendations

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/ \${TagKey} (p. 170)	
ListEventParticipants [permission only]	Grants permission to view the participants of an event	Read	Event* (p. 169)		
	aws:ResourceTag/ \${TagKey} (p. 170)				
ListEventScores [permission only]	Grants permission to view the scores of an event's players	Read	Event* (p. 169)		
	aws:ResourceTag/ \${TagKey} (p. 170)				
ListEvents [permission only]	Grants permission to List BugBust events	List		aws:ResourceTag/ \${TagKey} (p. 170)	
ListProfilingGroups [permission only]	Grants permission to view the profiling groups that were imported into an event for players to work on	Read	Event* (p. 169)		
	aws:ResourceTag/ \${TagKey} (p. 170)				
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* (p. 169)		
	aws:ResourceTag/ \${TagKey} (p. 170)				
ListTagsForResource [permission only]	Grants permission to lists tag for a Bugbust resource	Read	Event* (p. 169)		
	aws:ResourceTag/ \${TagKey} (p. 170)				
TagResource [permission only]	Grants permission to tag a Bugbust resource	Tagging	Event* (p. 169)		
	aws:TagKeys (p. 170)				
	aws:RequestTag/ \${TagKey} (p. 170)				
UntagResource [permission only]	Grants permission to untag a Bugbust resource	Tagging	Event* (p. 169)		
	aws:TagKeys (p. 170)				
	aws:RequestTag/ \${TagKey} (p. 170)				

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateEvent [permission only]	Grants permission to update a BugBust event	Write	Event* (p. 169)		codeguru-profiler:DescribeProfilingGroup codeguru-profiler>ListProfilingGroups codeguru-reviewer:DescribeCodeReview codeguru-reviewer>ListCodeReviews codeguru-reviewer>ListRecommendations codeguru-reviewer:TagResource codeguru-reviewer:UnTagResource
					aws:ResourceTag/\${TagKey} (p. 170)
UpdateWorkItem [permission only]	Grants permission to update a work item as claimed or unclaimed (bug or profiling group)	Write	Event* (p. 169)		codeguru-reviewer>ListRecommendations
					aws:ResourceTag/\${TagKey} (p. 170)
UpdateWorkItem [permission only]	Grants permission to update Adre event's work item (bug or profiling group)	Write	Event* (p. 169)		codeguru-reviewer>ListRecommendations
					aws:ResourceTag/\${TagKey} (p. 170)

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](#) (p. 167) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 170)

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters access based on the tags that are passed in the request	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters access based on the tags associated with the resource	String
<code>aws:TagKeys</code>	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 \(p. 170\)](#)
- [Resource types defined by AWS Certificate Manager \(p. 172\)](#)
- [Condition keys for AWS Certificate Manager \(p. 172\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 172)		
				aws:RequestTag/\${TagKey} (p. 172)	
				aws:TagKeys (p. 172)	
DeleteCertificate	Grants permission to delete a certificate and its associated private key	Write	certificate* (p. 172)		
DescribeCertificate	Grants permission to retrieve a certificate and its metadata	Read	certificate* (p. 172)		
ExportCertificate	Grants permission to export a private certificate issued by a private certificate authority (CA) for use anywhere	Read	certificate* (p. 172)		
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* (p. 172)		
ImportCertificate	Grants permission to import a 3rd party certificate into AWS Certificate Manager (ACM)	Write	certificate* (p. 172)		
				aws:RequestTag/\${TagKey} (p. 172)	
				aws:TagKeys (p. 172)	
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* (p. 172)		
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* (p. 172)		
				aws:RequestTag/\${TagKey} (p. 172)	
				aws:TagKeys (p. 172)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RenewCertificate	Grants permission to renew an eligible private certificate	Write	certificate* (p. 172)		
RequestCertificate	Grants permission to request a public or private certificate	Write		aws:RequestTag/\${TagKey} (p. 172) aws:TagKeys (p. 172)	
ResendValidationEmail	Grants permission to resend email to request domain ownership validation	Write	certificate* (p. 172)		
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* (p. 172)		

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 \(p. 170\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
certificate	<code>arn:\${Partition}:acm:\${Region}:\${Account}:certificate/\${CertificateId}</code>	aws:ResourceTag/\${TagKey} (p. 172)

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 [Available global condition keys](#).

Condition keys	Description	Type
aws:RequestTag/\${TagKey}	Filter access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/\${TagKey}	Filter 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 Certificate Manager Private Certificate Authority

AWS Certificate Manager 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 Certificate Manager Private Certificate Authority \(p. 173\)](#)
- [Resource types defined by AWS Certificate Manager Private Certificate Authority \(p. 175\)](#)
- [Condition keys for AWS Certificate Manager Private Certificate Authority \(p. 176\)](#)

Actions defined by AWS Certificate Manager 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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 ACM Private CA and its associated private key and configuration	Write		aws:RequestTag/\${TagKey} (p. 176) aws:TagKeys (p. 176)	
CreateCertificateAuthorityReport	Grants permission to create an audit report for an ACM Private CA	Write	certificate-authority* (p. 176)		
CreatePermission	Grants permission to create a permission for an ACM Private CA	Permissions	certificate-managementauthority* (p. 176)		

Service Authorization Reference
 Service Authorization Reference
 AWS Certificate Manager Private Certificate Authority

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteCertificateAuthority	Grants permission to delete an ACM Private CA and its associated private key and configuration	Write	certificate-authority* (p. 176)		
DeletePermission	Grants permission to delete a permission for an ACM Private CA	Permissions	certificate-management	certificate-authority* (p. 176)	
DeletePolicy	Grants permission to delete the policy for an ACM Private CA	Permissions	certificate-management	certificate-authority* (p. 176)	
DescribeCertificateAuthority	Grants permission to return a list of the configuration and status fields contained in the specified ACM Private CA	Read	certificate-authority* (p. 176)		
DescribeCertificateAuthorityAuditReport	Grants permission to return the status and audit report about an ACM Private CA audit report	Read	certificate-authority* (p. 176)		
GetCertificate	Grants permission to retrieve an ACM Private CA certificate and certificate chain for the certificate authority specified by an ARN	Read	certificate-authority* (p. 176)		
GetCertificateAuthority	Grants permission to retrieve an ACM Private CA certificate and certificate chain for the certificate authority specified by an ARN	Read	certificate-authority* (p. 176)		
GetCertificateAuthorityCSR	Grants permission to retrieve an ACM Private CA certificate signing request (CSR) for the certificate-authority specified by an ARN	Read	certificate-authority* (p. 176)		
GetPolicy	Grants permission to retrieve the policy on an ACM Private CA	Read	certificate-authority* (p. 176)		
ImportCertificate	Grants permission to import an SSL/TLS certificate into ACM Private CA for use as the CA certificate of an ACM Private CA	Write	certificate-authority* (p. 176)		
IssueCertificate	Grants permission to issue an ACM Private CA certificate	Write	certificate-authority* (p. 176)		acm-pca:TemplateArn (p. 176)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListCertificateAuthorities	Grants permission to retrieve a list of the ACM 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 ACM Private CA certificate authority	Read	certificate-authority* (p. 176)		
ListTags	Grants permission to list the tags that have been applied to the ACM Private CA certificate authority	Read	certificate-authority* (p. 176)		
PutPolicy	Grants permission to put a policy on an ACM Private CA	Permissions management	certificate-authority* (p. 176)		
RestoreCertificateAuthority	Grants permission to restore an ACM Private CA from the deleted state to the state it was in when deleted	Write	certificate-authority* (p. 176)		
RevokeCertificateAuthority	Grants permission to revoke a certificate issued by an ACM Private CA	Write	certificate-authority* (p. 176)		
TagCertificateAuthority	Grants permission to add one or more tags to an ACM Private CA	Tagging	certificate-authority* (p. 176)		
				aws:TagKeys (p. 176) aws:RequestTag/\${TagKey} (p. 176)	
UntagCertificateAuthority	Grants permission to remove one or more tags from an ACM Private CA	Tagging	certificate-authority* (p. 176)		
				aws:TagKeys (p. 176)	
UpdateCertificateAuthorityConfiguration	Grants permission to update the configuration of an ACM Private CA	Write	certificate-authority* (p. 176)		

Resource types defined by AWS Certificate Manager 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 \(p. 173\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 176)

Condition keys for AWS Certificate Manager Private Certificate Authority

AWS Certificate Manager 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 [Available global condition keys](#).

Condition keys	Description	Type
acm-pca:TemplateArn	Filters issue certificate requests based on the presence of TemplateArn in the request	String
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

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 \(p. 177\)](#)
- [Resource types defined by AWS Chatbot \(p. 178\)](#)
- [Condition keys for AWS Chatbot \(p. 179\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateChimeWebhookConfiguration	Grants permission to create an AWS Chatbot Chime Webhook Configuration	Write			
CreateSlackChannelConfiguration	Grants permission to create an AWS Chatbot Slack Channel Configuration	Write			
DeleteChimeWebhookConfiguration	Grants permission to delete an AWS Chatbot Chime Webhook Configuration	Write	ChatbotConfiguration* (p. 179)		
DeleteSlackChannelConfiguration	Grants permission to delete an AWS Chatbot Slack Channel Configuration	Write	ChatbotConfiguration* (p. 179)		
DeleteSlackUserIdentity	Grants permission to delete an AWS Chatbot Slack User Identity	Write			
DeleteSlackWorkAuthorization	Grants permission to delete the Slack Authorization associated 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			
DescribeSlackChannels	Grants permission to list all public Slack channels in the	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Slack workspace connected to the AWS Account onboarded with AWS Chatbot service				
DescribeSlackUser	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			
GetAccountPreferences	Grants permission to retrieve AWS Chatbot account preferences	Read			
GetSlackOauthParameters	Grants permission to generate OAuth parameters to request Slack OAuth code to be used by the AWS Chatbot service	Read			
RedeemSlackOAuthParameters	Grants permission to redeem previously generated parameters with Slack API, to acquire OAuth tokens to be used by the AWS Chatbot service	Write			
UpdateAccountPreferences	Grants permission to update AWS Chatbot account preferences	Write			
UpdateChimeWebhookConfiguration	Grants permission to update an AWS Chatbot Chime Webhook Configuration	Write	ChatbotConfiguration* (p. 179)		
UpdateSlackChannelConfiguration	Grants permission to update an AWS Chatbot Slack Channel Configuration	Write	ChatbotConfiguration* (p. 179)		

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 \(p. 177\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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}	

Condition keys for AWS Chatbot

Chatbot 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 [Available keys for conditions](#).

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 \(p. 179\)](#)
- [Resource types defined by Amazon Chime \(p. 202\)](#)
- [Condition keys for Amazon Chime \(p. 203\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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			
AddDomain	Grants permission to add a domain to your Amazon Chime account	Write			
AddOrUpdateGroup	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-user* (p. 202)		
			channel* (p. 202)		
			channel-flow* (p. 202)		
AssociatePhoneNumberWithUser	Grants permission to associate a phone number with an Amazon Chime user	Write			
AssociatePhoneNumberWithVoiceConnector	Grants permission to associate multiple phone numbers with an Amazon Chime Voice Connector	Write			
AssociatePhoneNumberWithVoiceConnectorGroup	Grants permission to associate multiple phone numbers with an Amazon Chime Voice Connector Group	Write			
AssociateSignInDelegates	Grants permission to associate the specified sign-in delegate groups with the specified Amazon Chime account	Write			
AuthorizeDirectory	Grants permission to authorize an Active Directory for your Amazon Chime Enterprise account	Write			
BatchCreateAttendees	Grants permission to create new attendees for an active Amazon Chime SDK meeting	Write	meeting* (p. 202)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchCreateChannelMembers	Grants permission to add multiple users to a channel	Write	app-instance-user* (p. 202)		
	channel* (p. 202)				
BatchCreateRoomMembers	Grants permission to batch add room members	Write			
BatchDeletePhoneNumbers	Grants permission to move up to 50 phone numbers to the deletion queue	Write			
BatchSuspendUsers	Grants permission to suspend up to 50 users from a Team or EnterpriseLWA Amazon Chime account	Write			
BatchUnsuspendUsers	Grants permission to remove the suspension from up to 50 previously suspended users for the specified Amazon Chime EnterpriseLWA account	Write			
BatchUpdatePhoneNumbers	Grants permission to update phone number details within the UpdatePhoneNumberRequestItem object for up to 50 phone numbers	Write			
BatchUpdateUsers	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* (p. 202)		
Connect	Grants permission to establish a web socket connection for app instance user to the messaging session endpoint	Write	app-instance-user* (p. 202)		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateApiKey	Grants permission to create a new SCIM access key for your Amazon Chime account and Okta configuration	Write			
CreateAppInstance	Grants permission to create an app instance under the AWS account	Write		aws:TagKeys (p. 203)	aws:RequestTag/ \${TagKey} (p. 203)
CreateAppInstanceUser	Grants permission to promote an AppInstanceUser to an AppInstanceAdmin	Write	app-instance* (p. 202)		
			app-instance-user* (p. 202)		
CreateAppInstanceUser	Grants permission to create a user under an Amazon Chime AppInstance	Write		aws:TagKeys (p. 203)	aws:RequestTag/ \${TagKey} (p. 203)
CreateAttendee	Grants permission to create a new attendee for an active Amazon Chime SDK meeting	Write	meeting* (p. 202)		
CreateBot	Grants permission to create a bot for an Amazon Chime Enterprise account	Write			
CreateBotMember	Grants permission to add a bot to a chat room in your 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 under the AWS account	Write	app-instance-user* (p. 202)		
				aws:TagKeys (p. 203)	aws:RequestTag/ \${TagKey} (p. 203)
CreateChannelBan	Grants permission to ban a user from a channel	Write	app-instance-user* (p. 202)		
				channel* (p. 202)	
CreateChannelFlow	Grants permission to create a channel flow for an app instance under the AWS account	Write	app-instance* (p. 202)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys (p. 203) aws:RequestTag/\${TagKey} (p. 203)	
CreateChannelMember	Grants permission to add a user to a channel	Write	app-instance-user* (p. 202) channel* (p. 202)		
CreateChannelModerator	Grants permission to create a channel moderator	Write	app-instance-user* (p. 202) channel* (p. 202)		
CreateMediaCapturePipeline	Grants permission to create a media capture pipeline	Write		aws:TagKeys (p. 203) aws:RequestTag/\${TagKey} (p. 203)	
CreateMeeting	Grants permission to create a new Amazon Chime SDK meeting in the specified media Region, with no initial attendees	Write		aws:RequestTag/\${TagKey} (p. 203) aws:TagKeys (p. 203)	
CreateMeetingDialInNumber	Grants permission to call a phone number to join the specified Amazon Chime SDK meeting	Write	meeting* (p. 202)		
CreateMeetingWithAttendees	Grants permission to create a new Amazon Chime SDK meeting in the specified media Region, with a set of attendees	Write		aws:RequestTag/\${TagKey} (p. 203) aws:TagKeys (p. 203)	
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			
CreateRoom	Grants permission to create a room	Write			
CreateRoomMember	Grants permission to add a room member	Write			
CreateSipMediaApplication	Grants permission to create an Amazon Chime SIP media application under the administrator's AWS account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSipMediaApplication	Grants permission to create an outboundCall for Amazon Chime SIP media application under the administrator's AWS account	Write			
CreateSipRule	Grants permission to create an Amazon Chime SIP rule under the administrator's AWS account	Write			
CreateUser	Grants permission to create a user under the specified Amazon Chime account	Write			
CreateVoiceConnector	Grants permission to create an Amazon Chime Voice Connector under the administrator's AWS account	Write			
CreateVoiceConnectorGroup	Grants permission to create an Amazon Chime Voice Connector Group under the administrator's AWS account	Write			
DeleteAccount	Grants permission to delete the specified Amazon Chime account	Write			
DeleteAccountOpener	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* (p. 202)		
DeleteAppInstanceAdmin	Grants permission to demote an AppInstanceAdmin to an AppInstanceUser	Write	app-instance* (p. 202)	app-instance-user* (p. 202)	
DeleteAppInstanceDataStreaming	Grants permission to disable data streaming for the app instance		app-instance* (p. 202)		
DeleteAppInstanceUser	Grants permission to delete an AppInstanceUser	Write	app-instance-user* (p. 202)		

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* (p. 202)		
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-user* (p. 202)		
			channel* (p. 202)		
DeleteChannelBan	Grants permission to remove a user from a channel's ban list	Write	app-instance-user* (p. 202)		
			channel* (p. 202)		
DeleteChannelFlow	Grants permission to delete a channel flow	Write	channel* (p. 202)		
DeleteChannelMember	Grants permission to remove a member from a channel	Write	app-instance-user* (p. 202)		
			channel* (p. 202)		
DeleteChannelMessage	Grants permission to delete a message	Write	app-instance-user* (p. 202)		
			channel* (p. 202)		
DeleteChannelModerator	Grants permission to delete a moderator	Write	app-instance-user* (p. 202)		
			channel* (p. 202)		
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			
DeleteEventsConfig	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* (p. 203)		
DeleteMeeting	Grants permission to delete the specified Amazon Chime SDK meeting	Write	meeting* (p. 202)		
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			
DeleteRoom	Grants permission to delete a room	Write			
DeleteRoomMember	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			
DeleteSipRule	Grants permission to delete Amazon Chime SIP rule under the administrator's AWS account	Write			
DeleteVoiceConnector	Grants permission to delete the specified Amazon Chime Voice Connector	Write			
DeleteVoiceConnectorEmergencyCallingConfiguration	Grants permission to delete emergency calling configuration for the specified Amazon Chime Voice Connector	Write			
DeleteVoiceConnectorGroup	Grants permission to delete the specified Amazon Chime Voice Connector Group	Write			
DeleteVoiceConnectorRegion	Grants permission to delete the region settings for the specified Amazon Chime Voice Connector	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVoiceConnectorProxyConfig	Grants permission to delete proxy configuration for the specified Amazon Chime Voice Connector	Write			
DeleteVoiceConnectorStreamingConfiguration	Grants permission to delete streaming configuration for the specified Amazon Chime Voice Connector	Write			
DeleteVoiceConnectorTerminationSettings	Grants permission to delete the termination settings for the specified Amazon Chime Voice Connector	Write			
DeleteVoiceConnectorTerminationCredentials	Grants permission to delete SIP termination credentials for the specified Amazon Chime Voice Connector	Write			
DeregisterAppInstanceEndpointPoint	Grants permission to deregister an endpoint point app instance user	Write	app-instance-user* (p. 202)		
DescribeAppInstanceDetails	Grants permission to get the full details of an AppInstance	Read	app-instance* (p. 202)		
DescribeAppInstanceAdminDetails	Grants permission to get the full details of an AppInstanceAdmin	Read	app-instance* (p. 202)		
			app-instance-user* (p. 202)		
DescribeAppInstanceUserDetails	Grants permission to get the full details of an AppInstanceUser	Read	app-instance-user* (p. 202)		
DescribeAppInstanceEndpointRegisters	Grants permission to describe an endpoint registered for an app instance user	Read	app-instance-user* (p. 202)		
DescribeChannel	Grants permission to get the full details of a channel	Read	app-instance-user* (p. 202)		
			channel* (p. 202)		
DescribeChannelBanDetails	Grants permission to get the full details of a channel ban	Read	app-instance-user* (p. 202)		
			channel* (p. 202)		
DescribeChannelFlowDetails	Grants permission to get the full details of a channel flow	Read	channel-flow* (p. 202)		

Service Authorization Reference
Service Authorization Reference
Amazon Chime

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeChannelMembership	Grants permission to get the full details of a channel membership	Read	app-instance-user* (p. 202)		
	channel* (p. 202)				
DescribeChannelMembershipForAppInstanceUser	Grants permission to get the details of a channel based on the membership of the specified AppInstanceUser	Read	app-instance-user* (p. 202)		
	channel* (p. 202)				
DescribeChannelModerator	Grants permission to get the full details of a channel moderated by the specified AppInstanceUser	Read	app-instance-user* (p. 202)		
	channel* (p. 202)				
DescribeChannelModeratorDetails	Grants permission to get the full details of a single ChannelModerator	Read	app-instance-user* (p. 202)		
	channel* (p. 202)				
DisassociateChannelFlow	Grants permission to disassociate a flow from a channel	Write	app-instance-user* (p. 202)		
	channel* (p. 202)				
	channel-flow* (p. 202)				
DisassociatePhoneNumber	Grants permission to disassociate the primary provisioned number from the specified Amazon Chime user	Write			
DisassociatePhoneNumberFromMultipleConnectors	Grants permission to disassociate multiple phone numbers from the specified Amazon Chime Voice Connector	Write			
DisassociatePhoneNumberFromMultipleConnectorGroups	Grants permission to disassociate multiple phone connector group numbers from the specified Amazon Chime Voice Connector Group	Write			
DisassociateSigninDelegateGroups	Grants permission to disassociate the specified sign-in delegate groups from the specified Amazon Chime account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
GetAccountResourceDetails	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 OpenIdConfig details and OpenIdConfig attributes for your Amazon Chime account	Read			
GetAppInstanceRetentionSettings	Grants permission to get retention settings for an app instance	Read	app-instance* (p. 202)		
GetAppInstanceStreamingConfigurations	Grants permission to get the streaming configurations for an app instance	Read	app-instance* (p. 202)		
GetAttendee	Grants permission to get attendee details for a specified meeting ID and attendee ID	Read	meeting* (p. 202)		
GetBot	Grants permission to retrieve details for the specified bot	Read			
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-user* (p. 202) channel* (p. 202)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetChannelMessageDetails	Grants permission to get the full details of a channel message	Read	app-instance-user* (p. 202)		
	channel* (p. 202)				
GetChannelMessageStatus	Grants permission to get the status of a channel message	Read	app-instance-user* (p. 202)		
	channel* (p. 202)				
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			
GetGlobalSetting	Grants permission to get global settings related to Amazon Chime for the AWS account	Read			
GetMediaCaptureExisting	Grants permission to get an existing media capture pipeline	Read	media-pipeline* (p. 203)		
GetMeeting	Grants permission to get the meeting record for a specified meeting ID	Read	meeting* (p. 202)		
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			
GetPhoneNumber	Grants permission to get details for the specified phone number	Read			
GetPhoneNumberOrder	Grants permission to get details for the specified phone number order	Read			
GetPhoneNumberSettings	Grants permission to get phone numbers settings related to Amazon Chime for the AWS account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetProxySession	Grants permission to get details of the specified proxy session for the specified Amazon Chime Voice Connector	Read			
GetRetentionSettings	Grants permission to retrieve the retention settings for the specified Amazon Chime account	Read			
GetRoom	Grants permission to retrieve a room	Read			
GetSipMediaApplicationDetails	Grants permission to get details of Amazon Chime SIP media application under the administrator's AWS account	Read			
GetSipMediaApplicationLoggingConfigurationSettings	Grants permission to get logging configuration settings for Amazon Chime SIP media application under the administrator's AWS account	Read			
GetSipRule	Grants permission to get details of Amazon Chime SIP rule under the administrator's AWS account	Read			
GetTelephonyLimits	Grants permission to get telephony limits for the AWS account	Read			
 GetUser	Grants permission to get details for the specified user ID	Read			
 GetUserActivityReportSummary	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			

Service Authorization Reference
Service Authorization Reference
Amazon Chime

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetVoiceConnectorEmergencyCallingConfiguration	Grants permission to get details of the emergency calling configuration for the specified Amazon Chime Voice Connector	Read			
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			
GetVoiceConnectorOrigination	Grants permission to get details of the origination settings for the specified Amazon Chime Voice Connector	Read			
GetVoiceConnectorProxy	Grants permission to get details of the proxy configuration for the specified Amazon Chime Voice Connector	Read			
GetVoiceConnectorStreamingConfiguration	Grants permission to get details of the streaming configuration for the specified Amazon Chime Voice Connector	Read			
GetVoiceConnectorTermination	Grants permission to get details of the termination settings for the specified Amazon Chime Voice Connector	Read			
GetVoiceConnectorTerminationHealth	Grants permission to get details of the termination health for the specified Amazon Chime Voice Connector	Read			
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			
ListAccountUsage	Grants permission to list Amazon Chime account usage reporting data	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
ListAppInstanceAdministrators	Grants permission to list Administrators in the app instance	List	app-instance* (p. 202)		
			app-instance-user* (p. 202)		
ListAppInstanceUserEndpoints	Grants permission to list the UserEndpoints registered for an app instance user	List	app-instance-user* (p. 202)		
ListAppInstanceUsers	Grants permission to list all AppInstanceUsers created under a single app instance	List	app-instance-user* (p. 202)		
ListInstances	Grants permission to list all Amazon Chime app instances created under a single AWS account	List	app-instance* (p. 202)		
ListAttendeeTags	Grants permission to list the tags applied to an Amazon Chime SDK attendee resource	List	meeting* (p. 202)		
ListAttendees	Grants permission to list up to 100 attendees for a specified Amazon Chime SDK meeting	List	meeting* (p. 202)		
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
ListCallingRegions	Grants permission to list the calling regions available for the administrator's AWS account	List			
ListChannelBans	Grants permission to list all the users banned from a particular channel	List	app-instance-user* (p. 202)		
			channel* (p. 202)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListChannelFlows	Grants permission to list all the Channel Flows created under a single Chime AppInstance	List	channel-flow* (p. 202)		
ListChannelMembers	Grants permission to list all channel memberships in a channel	List	app-instance-user* (p. 202)		
			channel* (p. 202)		
ListChannelMemberChannels	Grants permission to list all the channels that a particular AppInstanceUser is a part of	List	app-instance-user* (p. 202)		
ListChannelMessages	Grants permission to list all the messages in a channel	Read	app-instance-user* (p. 202)		
			channel* (p. 202)		
ListChannelModerators	Grants permission to list all the moderators for a channel	List	app-instance-user* (p. 202)		
			channel* (p. 202)		
ListChannels	Grants permission to list all the Channels created under a single Chime AppInstance	List	app-instance-user* (p. 202)		
			channel* (p. 202)		
ListChannelsAssociatedFlows	Grants permission to list all the Channel Flows created under a single Chime AppInstance	List	channel-flow* (p. 202)		
ListChannelsModeratedBy	Grants permission to list all channels moderated by an app instance user	List	app-instance-user* (p. 202)		
ListDelegates	Grants permission to list account delegate information associated with your Amazon Chime account	List			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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* (p. 202)		
ListMeetings	Grants permission to list up to 100 active Amazon Chime SDK meetings	List			
ListMeetingsReported	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			
ListPhoneNumberRegistrations	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			
ListRoomMemberships	Grants permission to list all room members	List			
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			
ListSupportedPhoneNumbersInCountries	Grants permission to list the phone numbers in countries supported by the AWS account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to list the tags applied to an Amazon Chime resource	Read	channel (p. 202)		
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			
ListVoiceConnectors	Grants permission to list the Amazon Chime Voice Connectors under the administrator's AWS account	List			
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* (p. 202)		
PutAppInstanceStreamingConfig	Grants permission to configure data streaming for the app instance	Write	app-instance* (p. 202)		
PutChannelMembershipPreferences	Grants permission to put the preferences for channel membership	Write	app-instance-user* (p. 202)	channel* (p. 202)	
PutEventsConfiguration	Grants permission to update details for an events configuration for a bot to receive outgoing events	Write			
PutRetentionSettings	Grants permission to create or update retention settings for the specified Amazon Chime account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutSipMediaApplicationLoggingConfiguration	Grants permission to update logging configuration settings for Amazon Chime SIP media application under the administrator's AWS account	Write			
PutVoiceConnectorEmergencyCallingConfiguration	Grants permission to add emergency calling configuration for the specified Amazon Chime Voice Connector	Write			
PutVoiceConnectorLoggingConfiguration	Grants permission to add logging configuration for the specified Amazon Chime Voice Connector	Write			logs>CreateLogDelivery logs>CreateLogGroup logs>DeleteLogDelivery logs>DescribeLogGroups logs>GetLogDelivery logs>ListLogDeliveries
PutVoiceConnectorOrigination	Grants permission to update the origination settings for the specified Amazon Chime Voice Connector	Write			
PutVoiceConnectorProxyConfiguration	Grants permission to add proxy configuration for the specified Amazon Chime Voice Connector	Write			
PutVoiceConnectorStreamingConfiguration	Grants permission to add streaming configuration for the specified Amazon Chime Voice Connector	Write			
PutVoiceConnectorTermination	Grants permission to update the termination settings for the specified Amazon Chime Voice Connector	Write			
PutVoiceConnectorTerminationCredentials	Grants permission to add SIP termination credentials for the specified Amazon Chime Voice Connector	Write			
RedactChannelMessageContent	Grants permission to redact message content	Write	app-instance-user* (p. 202) channel* (p. 202)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
RegisterAppInstanceUser	Grants permission to register the endpoint for an app instance user	Write	app-instance-user* (p. 202)		
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			
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 deletion queue back to the phone number inventory	Write			
RetrieveDataExport	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			
SendChannelMessage	Grants permission to send a message to a particular channel that the member is a part of	Write	app-instance-user* (p. 202) channel* (p. 202)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartDataExport	Grants permission to submit the "Request attachments" request	Write			
StartMeetingTranscription	Grants permission to start transcription for a meeting	Write			
StopMeetingTranscription	Grants permission to stop transcription for a meeting	Write			
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* (p. 202)		
TagMeeting	Grants permission to apply the specified tags to the specified Amazon Chime SDK meeting	Tagging	meeting* (p. 202) aws:TagKeys (p. 203) aws:RequestTag/ \${TagKey} (p. 203) aws:ResourceTag/ \${TagKey} (p. 203)		
			aws:TagKeys (p. 203) aws:RequestTag/ \${TagKey} (p. 203) aws:ResourceTag/ \${TagKey} (p. 203)		
			aws:TagKeys (p. 203) aws:RequestTag/ \${TagKey} (p. 203) aws:ResourceTag/ \${TagKey} (p. 203)		
			aws:TagKeys (p. 203) aws:RequestTag/ \${TagKey} (p. 203) aws:ResourceTag/ \${TagKey} (p. 203)		
TagResource	Grants permission to apply the specified tags to the specified Amazon Chime resource	Tagging	channel (p. 202)		
media-pipeline (p. 203)					
aws:TagKeys (p. 203) aws:RequestTag/ \${TagKey} (p. 203) aws:ResourceTag/ \${TagKey} (p. 203)					
aws:TagKeys (p. 203) aws:RequestTag/ \${TagKey} (p. 203) aws:ResourceTag/ \${TagKey} (p. 203)					
UnauthorizeDirectory	Grants permission to unauthorized 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* (p. 202)		
UntagMeeting	Grants permission to untag the specified tags from the specified Amazon Chime SDK meeting	Tagging	meeting* (p. 202)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagResource	Grants permission to untag the specified tags from the specified Amazon Chime resource	Tagging	channel (p. 202)		
			media-pipeline (p. 203)		
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			
UpdateAccountRetention	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			
UpdateAppInstance	Grants permission to update AppInstance metadata	Write	app-instance* (p. 202)		
UpdateAppInstanceDetails	Grants permission to update the details for an AppInstanceUser	Write	app-instance-user* (p. 202)		
UpdateAppInstanceEndpointRegistration	Grants permission to update an endpoint registered for an app instance user	Write	app-instance-user* (p. 202)		
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-user* (p. 202)		
	channel* (p. 202)				
UpdateChannelFlow	Grants permission to update a channel flow	Write	channel-flow* (p. 202)		
UpdateChannelMessageContent	Grants permission to update the content of a message	Write	app-instance-user* (p. 202)		
	channel* (p. 202)				

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateChannelRetentionStamp	Grants permission to set the channel retention stamp to the point when a user last read messages in a channel	Write	app-instance-user* (p. 202)		
			channel* (p. 202)		
UpdateGlobalSettings	Grants permission to update the global settings related to Amazon Chime for the AWS account	Write			
UpdatePhoneNumber	Grants permission to update phone number details for the specified phone number	Write			
UpdatePhoneNumberSetting	Grants permission to update phone setting 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			
UpdateRoom	Grants permission to update a room	Write			
UpdateRoomMembership	Grants permission to update membership role	Write			
UpdateSipMediaApplicationProperties	Grants permission to update properties of Amazon Chime SIP media application under the administrator's AWS account	Write			
UpdateSipMediaApplicationAmazonCall	Grants permission to update an Amazon Call chime SIP media application call under the administrator's AWS account	Write			
UpdateSipRule	Grants permission to update properties of Amazon Chime SIP rule under the administrator's AWS account	Write			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
UpdateVoiceConnectorGroup	Grants permission to update Amazon Chime Voice Connector Group details for the specified Amazon Chime Voice Connector Group	Write			
ValidateAccount	Grants permission to validate the account resource in your Amazon Chime account	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 \(p. 179\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
meeting	arn:\${Partition}:chime::\${AccountId}:meeting/\${MeetingId}	aws:ResourceTag/\${TagKey} (p. 203)
app-instance	arn:\${Partition}:chime:\${Region}: \${AccountId}:app-instance/\${AppInstanceId}	aws:ResourceTag/\${TagKey} (p. 203)
app-instance-user	arn:\${Partition}:chime:\${Region}: \${AccountId}:app-instance/\${AppInstanceId}/user/\${AppInstanceUserId}	aws:ResourceTag/\${TagKey} (p. 203)
channel	arn:\${Partition}:chime:\${Region}: \${AccountId}:app-instance/\${AppInstanceId}/channel/\${ChannelId}	aws:ResourceTag/\${TagKey} (p. 203)
channel-flow	arn:\${Partition}:chime:\${Region}: \${AccountId}:app-instance/\${AppInstanceId}/channel-flow/\${ChannelFlowId}	aws:ResourceTag/\${TagKey} (p. 203)

Resource types	ARN	Condition keys
media-pipeline	<code>arn:\${Partition}:chime:\${Region}:\${AccountId}:media-pipeline/\${MediaPipelineId}</code>	aws:ResourceTag/\${TagKey} (p. 203)

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 [Available global condition 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 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 \(p. 203\)](#)
- [Resource types defined by AWS Cloud Control API \(p. 204\)](#)
- [Condition keys for AWS Cloud Control API \(p. 204\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 <code>resource</code> 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			
GetResourceRequest	Grants permission to get <code>resource</code> requests in your account	Read			
ListResourceRequest	Grants permission to list <code>resource</code> 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 [Available keys for conditions](#).

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 \(p. 205\)](#)
- [Resource types defined by Amazon Cloud Directory \(p. 211\)](#)
- [Condition keys for Amazon Cloud Directory \(p. 211\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 211)		
ApplySchema	Grants permission to copy input published schema into Directory with same name and version as that of published schema	Write	directory* (p. 211)		
			publishedSchema* (p. 211)		
AttachObject	Grants permission to attach an existing object to another existing object	Write	directory* (p. 211)		
AttachPolicy	Grants permission to attach a policy object to any other object	Write	directory* (p. 211)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AttachToIndex	Grants permission to attach the specified object to the specified index	Write	directory* (p. 211)		
AttachTypedLink	Grants permission to attach a typed link b/w a source & target object reference	Write	directory* (p. 211)		
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* (p. 211)		
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* (p. 211)		
CreateDirectory	Grants permission to create a Directory by copying the published schema into the directory	Write	publishedSchema* (p. 211)		
CreateFacet	Grants permission to create a new Facet in a schema	Write	appliedSchema* (p. 211)		
			developmentSchema* (p. 211)		
CreateIndex	Grants permission to create an index object	Write	directory* (p. 211)		
CreateObject	Grants permission to create an object in a Directory	Write	directory* (p. 211)		
CreateSchema	Grants permission to create a new schema in a development state	Write			
CreateTypedLink	Grants permission to create a new Typed Link facet in a schema	Write	appliedSchema* (p. 211)		
			developmentSchema* (p. 211)		
DeleteDirectory	Grants permission to delete a directory. Only disabled directories can be deleted	Write	directory* (p. 211)		
DeleteFacet	Grants permission to delete a given Facet. All attributes and Rules associated with the facet will be deleted	Write	developmentSchema* (p. 211)		
DeleteObject	Grants permission to delete an object and its associated attributes	Write	directory* (p. 211)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteSchema	Grants permission to delete a given schema	Write	developmentSchema* (p. 211)		
			publishedSchema* (p. 211)		
DeleteTypedLinkFacet	Grants permission to delete a given TypedLink Facet. All attributes and Rules associated with the facet will be deleted	Write	developmentSchema* (p. 211)		
DetachFromIndex	Grants permission to detach the specified object from the specified index	Write	directory* (p. 211)		
DetachObject	Grants permission to detach a given object from the parent object	Write	directory* (p. 211)		
DetachPolicy	Grants permission to detach a policy from an object	Write	directory* (p. 211)		
DetachTypedLink	Grants permission to detach a given typed link b/w given source and target object reference	Write	directory* (p. 211)		
DisableDirectory	Grants permission to disable the specified directory	Write	directory* (p. 211)		
EnableDirectory	Grants permission to enable the specified directory	Write	directory* (p. 211)		
GetAppliedSchema	Grants permission to return current applied schema version ARN, including the minor version in use	Read	appliedSchema* (p. 211)		
GetDirectory	Grants permission to retrieve metadata about a directory	Read	directory* (p. 211)		
GetFacet	Grants permission to get details of the Facet, such as Facet Name, Attributes, Rules, or ObjectType	Read	appliedSchema* (p. 211)		
			developmentSchema* (p. 211)		
			publishedSchema* (p. 211)		
GetLinkAttributes	Grants permission to retrieve attributes that are associated with a typed link	Read	directory* (p. 211)		
GetObjectAttributes	Grants permission to retrieve attributes within a facet that are associated with an object	Read	directory* (p. 211)		
GetObjectInformation	Grants permission to retrieve metadata about an object	Read	directory* (p. 211)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSchemaAsJson	Grants permission to retrieve a JSON representation of the schema	Read	appliedSchema* (p. 211)		
	developmentSchema* (p. 211)				
	publishedSchema* (p. 211)				
GetTypedLinkFacetIdentityAttributes	Grants permission to return information associated with a given typed link facet	Read	appliedSchema* (p. 211)		
	developmentSchema* (p. 211)				
	publishedSchema* (p. 211)				
ListAppliedSchemas	Grants permission to list schemas applied to a directory	List	directory* (p. 211)		
ListAttachedIndices	Grants permission to list indices attached to an object	Read	directory* (p. 211)		
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* (p. 211)		
	developmentSchema* (p. 211)				
	publishedSchema* (p. 211)				
ListFacetNames	Grants permission to retrieve the names of facets that exist in a schema	Read	appliedSchema* (p. 211)		
developmentSchema* (p. 211)					
publishedSchema* (p. 211)					
ListIncomingTypedLinks	Grants permission to return a paginated list of all incoming TypedLinks for a given object	Read	directory* (p. 211)		
ListIndex	Grants permission to list objects attached to the specified index	Read	directory* (p. 211)		
ListManagedSchemaVersions	Grants permission to list the major/minor 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* (p. 211)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListObjectChildren	Grants permission to return a paginated list of child objects associated with a given object	Read	directory* (p. 211)		
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* (p. 211)		
ListObjectParents	Grants permission to list parent objects associated with a given object in pagination fashion	Read	directory* (p. 211)		
ListObjectPolicies	Grants permission to return policies attached to an object in pagination fashion	Read	directory* (p. 211)		
ListOutgoingTypedLinks	Grants permission to return a paginated list of all outgoing TypedLinks for a given object	Read	directory* (p. 211)		
ListPolicyAttachments	Grants permission to return all of the ObjectIdentifiers to which a given policy is attached	Read	directory* (p. 211)		
ListPublishedSchemas	Grants permission to retrieve published schema ARNs	List			
ListTagsForResource	Grants permission to return tags for a resource	Read	directory* (p. 211)		
ListTypedLinkFacetAttributes	Grants permission to return a paginated list of attributes associated with typed link facet	Read	appliedSchema* (p. 211)		
ListTypedLinkFacetNames	Grants permission to return a paginated list of typed link facet names that exist in a schema		developmentSchema* (p. 211)		
ListTypedLinkFacetNames			publishedSchema* (p. 211)		
LookupPolicy	Grants permission to list all policies from the root of the Directory to the object specified	Read	directory* (p. 211)		
PublishSchema	Grants permission to publish a development schema with a version	Write	developmentSchema* (p. 211)		
PutSchemaFromJson	Grants permission to update schema using JSON upload. Only available for development schemas	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RemoveFacetFromObject	Grants permission to remove the specified facet from the specified object	Write	directory* (p. 211)		
TagResource	Grants permission to add tags to a resource	Tagging	directory* (p. 211)		
UntagResource	Grants permission to remove tags from a resource	Tagging	directory* (p. 211)		
UpdateFacet	Grants permission to add/update/delete existing Attributes, Rules, or ObjectType of a Facet	Write	appliedSchema* (p. 211) developmentSchema* (p. 211)		
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* (p. 211)		
UpdateObjectAttributes	Grants permission to update a given object's attributes	Write	directory* (p. 211)		
UpdateSchema	Grants permission to update the schema name with a new name	Write	developmentSchema* (p. 211)		
UpdateTypedLinkUpdate	Grants permission to add/update/delete existing Attributes, Rules, identity attribute order of a TypedLink Facet	Write	developmentSchema* (p. 211)		
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* (p. 211) publishedSchema* (p. 211)		
UpgradePublishedSchema	Grants permission to upgrade a published schema under a new minor version revision using the current contents of DevelopmentSchemaArn	Write	developmentSchema* (p. 211) publishedSchema* (p. 211)		

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 \(p. 205\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
appliedSchema	<code>arn:\${Partition}:clouddirectory:\${Region}: \${Account}:directory/\${DirectoryId}/schema/\${SchemaName}/\${Version}</code>	
developmentSchema	<code>arn:\${Partition}:clouddirectory:\${Region}: \${Account}:schema/development/\${SchemaName}</code>	
directory	<code>arn:\${Partition}:clouddirectory:\${Region}: \${Account}:directory/\${DirectoryId}</code>	
publishedSchema	<code>arn:\${Partition}:clouddirectory:\${Region}: \${Account}:schema/published/\${SchemaName}/\${Version}</code>	

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 [Available keys for conditions](#).

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 \(p. 211\)](#)
- [Resource types defined by AWS Cloud Map \(p. 214\)](#)
- [Condition keys for AWS Cloud Map \(p. 214\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 (p. 214) aws:RequestTag/\${TagKey} (p. 214)	
CreatePrivateDnsNamespace	Grants permission to create a private namespace based on DNS, which will be visible only inside a specified Amazon VPC	Write		aws:TagKeys (p. 214) aws:RequestTag/\${TagKey} (p. 214)	
CreatePublicDnsNamespace	Grants permission to create a public namespace based on DNS, which will be visible on the internet	Write		aws:TagKeys (p. 214) aws:RequestTag/\${TagKey} (p. 214)	
CreateService	Grants permission to create a service	Write	namespace* (p. 214) servicediscovery:NamespaceArn (p. 215) aws:TagKeys (p. 214) aws:RequestTag/\${TagKey} (p. 214)		
DeleteNamespace	Grants permission to delete a specified namespace	Write	namespace* (p. 214)		
DeleteService	Grants permission to delete a specified service	Write	service* (p. 214)		
DeregisterInstance	Grants permission to delete the records and the health check, if any, that Amazon Route 53 created for the specified instance	Write	service* (p. 214) servicediscovery:ServiceArn (p. 215)		
DiscoverInstances	Grants permission to discover registered instances for a specified namespace and service	Read		servicediscovery:NamespaceName (p. 215) servicediscovery:ServiceName (p. 215)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetInstance	Grants permission to get information about a specified instance	Read			servicediscovery:ServiceArn (p. 215)
GetInstancesHealth	Grants permission to get the current health status (Healthy, Unhealthy, or Unknown) of one or more instances	Read			servicediscovery:ServiceArn (p. 215)
GetNamespace	Grants permission to get information about a namespace	Read	namespace* (p. 214)		
GetOperation	Grants permission to get information about a specific operation	Read			
GetService	Grants permission to get the settings for a specified service	Read	service* (p. 214)		
ListInstances	Grants permission to get summary information about the instances that were registered with a specified service	Read			servicediscovery:ServiceArn (p. 215)
ListNamespaces	Grants permission to get information about the namespaces	Read			
ListOperations	Grants permission to list operations that match the criteria that you specify	List			
ListServices	Grants permission to get settings for all the services that match specified filters	Read			
ListTagsForResource	Grants permission to lists tags for the specified resource	Read			
RegisterInstance	Grants permission to register an instance based on the settings in a specified service	Write	service* (p. 214)		servicediscovery:ServiceArn (p. 215)
TagResource	Grants permission to add one or more tags to the specified resource	Tagging			aws:TagKeys (p. 214) aws:RequestTag/\${TagKey} (p. 214)
UntagResource	Grants permission to remove one or more tags from the specified resource	Tagging			aws:TagKeys (p. 214) aws:RequestTag/\${TagKey} (p. 214)
UpdateHttpNamespace	Grants permission to update the settings for a HTTP namespace	Write	namespace* (p. 214)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateInstanceCustomHealth	Grants permission to update the <code>currentHealth</code> status for an instance that has a custom health check	Write			servicediscovery:ServiceArn (p. 215)
UpdatePrivateDnsSettings	Grants permission to update the <code>settings</code> for a private DNS namespace	Write	namespace* (p. 214)		
UpdatePublicDnsSettings	Grants permission to update the <code>settings</code> for a public DNS namespace	Write	namespace* (p. 214)		
UpdateService	Grants permission to update the settings in a specified service	Write	service* (p. 214)		

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](#) (p. 211) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
namespace	<code>arn:\${Partition}:servicediscovery:\${Region}:\${Account}:namespace/\${NamespaceId}</code>	aws:ResourceTag/\${TagKey} (p. 214)
service	<code>arn:\${Partition}:servicediscovery:\${Region}:\${Account}:service/\${ServiceId}</code>	aws:ResourceTag/\${TagKey} (p. 214)

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 [Available global condition 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	String

Condition keys	Description	Type
servicediscovery:NameArn	Filters access by specifying the Amazon Resource Name (ARN) for the related namespace	String
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	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 \(p. 215\)](#)
- [Resource types defined by AWS Cloud9 \(p. 219\)](#)
- [Condition keys for AWS Cloud9 \(p. 219\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 219)		
CreateEnvironment [permission only]	Grants permission to create an AWS Cloud9 development environment, launches an Amazon Elastic Compute Cloud (Amazon EC2) instance, and then hosts the environment on the instance	Write		cloud9:EnvironmentName (p. 219) cloud9:InstanceType (p. 219) cloud9:SubnetId (p. 219) cloud9:UserArn (p. 220) cloud9:OwnerArn (p. 220) aws:RequestTag/\${TagKey} (p. 219) aws:TagKeys (p. 219)	ec2:DescribeSubnets (p. 219) ec2:DescribeVpcs iam:CreateServiceLinkedRole (p. 219)
CreateEnvironmentMember [permission only]	Grants permission to add an environment member to an AWS Cloud9 development environment	Write	environment* (p. 219)		
				cloud9:UserArn (p. 220)	cloud9:EnvironmentId (p. 219) cloud9:Permissions (p. 220)
CreateEnvironmentSSH [permission only]	Grants permission to create an AWS Cloud9 SSH development environment	Write		cloud9:EnvironmentName (p. 219) cloud9:OwnerArn (p. 220) aws:RequestTag/\${TagKey} (p. 219) aws:TagKeys (p. 219)	
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* (p. 219)		
DeleteEnvironment [permission only]	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* (p. 219)		iam:CreateServiceLinkedRole (p. 219)
DeleteEnvironmentMember [permission only]	Grants permission to delete an environment member from an AWS Cloud9 development environment	Write	environment* (p. 219)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeEC2Remote [permission only]	Grants permission to get details about the connection to the EC2 development environment, including host, user, and port	Read	environment* (p. 219)		
DescribeEnvironment [permission only]	Grants permission to get information about environment members for an AWS Cloud9 development environment	Read	environment* (p. 219)	cloud9:UserArn (p. 220)	cloud9:EnvironmentId (p. 219)
DescribeEnvironment [permission only]	Grants permission to get status information for an AWS Cloud9 development environment	Read	environment* (p. 219)		
DescribeEnvironment [permission only]	Grants permission to get information about AWS Cloud9 development environments	Read	environment* (p. 219)		
DescribeSSHRemote [permission only]	Grants permission to get details about the connection to the SSH development environment, including host, user, and port	Read	environment* (p. 219)		
GetEnvironmentConfig [permission only]	Grants permission to get configuration information that's used to initialize the AWS Cloud9 IDE	Read	environment* (p. 219)		
GetEnvironmentAWSCode [permission only]	Grants permission to get the AWS Cloud9 IDE settings for a specified development environment	Read	environment* (p. 219)		
GetMembershipSettings [permission only]	Grants permission to get the AWS Cloud9 IDE settings for a specified environment member	Read	environment* (p. 219)		
 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 (p. 220)	
 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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to list tags for a cloud9 environment	Read	environment* (p. 219)		
ModifyTemporaryManagedTemporaryCredentials [permission only]	Grants permission to set AWS temporary credentials on the Amazon EC2 instance that's used by the AWS Cloud9 integrated development environment (IDE)	Write	environment* (p. 219)		
TagResource	Grants permission to add tags to a cloud9 environment	Tagging	environment* (p. 219)		
				aws:RequestTag/ \${TagKey} (p. 219)	aws:TagKeys (p. 219)
UntagResource	Grants permission to remove tags from a cloud9 environment	Tagging	environment* (p. 219)		
				aws:RequestTag/ \${TagKey} (p. 219)	aws:TagKeys (p. 219)
UpdateEnvironment	Grants permission to change the settings of an existing AWS Cloud9 development environment	Write	environment* (p. 219)		
UpdateEnvironmentMember	Grants permission to change the settings of an existing environment member for an AWS Cloud9 development environment	Write	environment* (p. 219)		
				cloud9:UserArn (p. 220)	cloud9:EnvironmentId (p. 219)
UpdateEnvironmentMemberAWSCodeCloud9IDE [permission only]	Grants permission to update the AWS Cloud9 IDE settings for a specified development environment	Write	environment* (p. 219)		
				cloud9:Permissions (p. 220)	
UpdateMemberAWSCodeCloud9IDE [permission only]	Grants permission to update the AWS Cloud9 IDE settings for a specified environment member	Write	environment* (p. 219)		
UpdateSSHRemoteDetails [permission only]	Grants permission to update details about the connection to the SSH development environment, including host, user, and port	Write	environment* (p. 219)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateUserSetting [permission only]	Grants permission to update IDE-specific settings of an AWS Cloud9 user	Write			
ValidateEnvironment [permission only]	Grants permission to validate the environment name during the process of creating an AWS Cloud9 development environment	Read			

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 \(p. 215\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
environment	<code>arn:\${Partition}:cloud9:\${Region}:\${Account}:environment:\${ResourceId}</code>	<code>aws:ResourceTag/\${TagKey}</code> (p. 219)

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 [Available global condition 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

Condition keys	Description	Type
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 \(p. 220\)](#)
- [Resource types defined by AWS CloudFormation \(p. 228\)](#)
- [Condition keys for AWS CloudFormation \(p. 228\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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				
BatchDescribeTypeConfiguration	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* (p. 228)		
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* (p. 228)		
CreateChangeSet	Grants permission to create a list of changes for a stack		stack* (p. 228)		
CreateStack	Grants permission to create a stack as specified in the template	Write	stack* (p. 228)		
	cloudformation:ResourceTypes (p. 229) cloudformation:ImportResourceTypes cloudformation:RoleArn (p. 229) cloudformation:StackPolicyUrl (p. 229) cloudformation:TemplateUrl (p. 229) aws:RequestTag/\${TagKey} (p. 228) aws:TagKeys (p. 228)				
CreateStackInstances	Grants permission to create stack instances for the specified accounts, within the specified regions	Write	stackset* (p. 228)		
			stackset-target (p. 228)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			type (p. 228)		
					cloudformation:TargetRegion (p. 229)
CreateStackSet	Grants permission to create a stackset as specified in the template	Write			cloudformation:RoleArn (p. 229) cloudformation:TemplateUrl (p. 229) aws:RequestTag/\${TagKey} (p. 228) aws:TagKeys (p. 228)
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			
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* (p. 228)		
					cloudformation:ChangeSetName (p. 229)
DeleteStack	Grants permission to delete a specified stack	Write	stack* (p. 228)		
					cloudformation:RoleArn (p. 229)
DeleteStackInstances	Grants permission to delete stack instances for the specified accounts, in the specified regions	Write	stackset* (p. 228)		
			stackset-target (p. 228)		
			type (p. 228)		
					cloudformation:TargetRegion (p. 229)
DeleteStackSet	Grants permission to delete a specified stackset	Write	stackset* (p. 228)		
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		Read	stack* (p. 228)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to return the description for the specified change set				cloudformation:ChangeSetName (p. 228)
DescribeChangeSetHistory	Grants permission to return the invocation information for the specified change set	Read	stack* (p. 228)		
					cloudformation:ChangeSetName (p. 228)
DescribePublisher	Grants permission to return information about a CloudFormation extension publisher	Read			
DescribeStackDriftInformation	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* (p. 228)		
DescribeStackInstances	Grants permission to return the stack instance that's associated with the specified stack set, AWS account, and region	Read	stackset* (p. 228)		
DescribeStackResources	Grants permission to return the description of the specified resource in the specified stack	Read	stack* (p. 228)		
DescribeStackResourceInformation	Grants permission to return drift information for the resources that have been checked for drift in the specified stack	Read	stack* (p. 228)		
DescribeStackResources	Grants permission to return AWS resource descriptions for running and deleted stacks	Read	stack* (p. 228)		
DescribeStackSets	Grants permission to return the description of the specified stack set	Read	stackset* (p. 228)		
DescribeStackSetOperations	Grants permission to return the description of the specified stack set operation	Read	stackset* (p. 228)		
DescribeStacks	Grants permission to return the description for the specified stack	List	stack* (p. 228)		
DescribeType	Grants permission to return information about the CloudFormation type requested	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeTypeRegistration	Grants permission to return information about the registration process for a CloudFormation type	Read			
DetectStackDrift	Grants permission to detect whether a stack's actual configuration differs, or has drifted, from its expected configuration, as defined in the stack template and any values specified as template parameters	Read	stack* (p. 228)		
DetectStackResourceDrift	Grants permission to return information about whether a resource's actual configuration differs, or has drifted, from its expected configuration, as defined in the stack template and any values specified as template parameters	Read	stack* (p. 228)		
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* (p. 228)		
EstimateTemplateCost	Grants permission to return the estimated monthly cost of a template	Read			
ExecuteChangeSet	Grants permission to update a stack using the input information that was provided when the specified change set was created	Write	stack* (p. 228)		
					cloudformation:ChangeSetName (p. 228)
GetStackPolicy	Grants permission to return the stack policy for a specified stack	Read	stack* (p. 228)		
GetTemplate	Grants permission to return the template body for a specified stack	Read	stack* (p. 228)		
GetTemplateSummary	Grants permission to return information about a new or existing template	Read	stack (p. 228)		
				stackset (p. 228)	
ImportStacksToStackSet	Grants permission to enable users to import existing stacks to a new or existing stackset	Write	stackset* (p. 228)		

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* (p. 228)		
ListExports	Grants permission to list all exported output values in the account and region in which you call this action	List			
ListImports	Grants permission to list all stacks that are importing an exported output value	List			
ListStackInstances	Grants permission to return summary information about stack instances that are associated with the specified stack set	List	stackset* (p. 228)		
ListStackResources	Grants permission to return descriptions of all resources of the specified stack	List	stack* (p. 228)		
ListStackSetOperationsSummary	Grants permission to return summary information about the results of a stack set operation	List	stackset* (p. 228)		
ListStackSetOperations	Grants permission to return summary information about operations performed on a stack set	List	stackset* (p. 228)		
ListStackSets	Grants permission to return summary information about stack sets that are associated with the user	List	stackset* (p. 228)		
ListStacks	Grants permission to return the summary information for stacks whose status matches the specified StackStatusFilter	List			
ListTypeRegistrations	Grants permission to list CloudFormation type registration attempts	List			
ListTypeVersions	Grants permission to list versions of a particular CloudFormation type	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 progress of a handler	Write	stack* (p. 228)		
RegisterPublisher	Grants permission to register an account as a publisher of public extensions in the CloudFormation registry	Write			
.RegisterType	Grants permission to register a new CloudFormation type	Write			
RollbackStack	Grants permission to rollback the stack to the last stable state	Write	stack* (p. 228) cloudformation:RoleArn (p. 229)		
SetStackPolicy	Grants permission to set a stack policy for a specified stack	Permissions management	stack* (p. 228) cloudformation:StackPolicyUrl (p. 229)		
SetTypeConfiguration	Grants permission to set configuration data for a registered CloudFormation extension, in the given account and region	Write			
SetTypeDefaultVersion	Grants permission to set which revision 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* (p. 228)		
StopStackSetOperation	Grants permission to stop an in-progress operation on a stack set and its associated stack instances	Write	stackset* (p. 228)		
TagResource	Grants permission to tag cloudformation resources	Tagging	changeset (p. 228) stack (p. 228) stackset (p. 228)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TestType	Grants permission to test a registered extension to make sure it meets all necessary requirements for being published in the CloudFormation registry	Write			
UntagResource	Grants permission to untag cloudformation resources	Tagging	changeset (p. 228)		
			stack (p. 228)		
			stackset (p. 228)		
UpdateStack	Grants permission to update a stack as specified in the template	Write	stack* (p. 228)		
			cloudformation:ResourceTypes (p. 229)		
			cloudformation:RoleArn (p. 229)		
			cloudformation:StackPolicyUrl (p. 229)		
			cloudformation:TemplateUrl (p. 229)		
			aws:RequestTag/\${TagKey} (p. 228)		
			aws:TagKeys (p. 228)		
UpdateStackInstances	Grants permission to update the parameter values for stack instances for the specified accounts, within the specified regions	Write	stackset* (p. 228)		
			stackset-target (p. 228)		
			type (p. 228)		
			cloudformation:TargetRegion (p. 229)		
UpdateStackSet	Grants permission to update a stackset as specified in the template	Write	stackset* (p. 228)		
			stackset-target (p. 228)		
			type (p. 228)		
			cloudformation:RoleArn (p. 229)		
			cloudformation:TemplateUrl (p. 229)		
			cloudformation:TargetRegion (p. 229)		
			aws:RequestTag/\${TagKey} (p. 228)		
			aws:TagKeys (p. 228)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateTerminationProtection	Grants permission to update Termination protection for the specified stack	Write	stack* (p. 228)		
ValidateTemplate	Grants permission to validate a specified template	Read			

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 \(p. 220\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 228)
stack	arn:\${Partition}:cloudformation:\${Region}: \${Account}:stack/\${StackName}/\${Id}	aws:ResourceTag/\${TagKey} (p. 228)
stackset	arn:\${Partition}:cloudformation:\${Region}: \${Account}:stackset/\${StackSetName}:\${Id}	aws:ResourceTag/\${TagKey} (p. 228)
stackset-target	arn:\${Partition}:cloudformation:\${Region}: \${Account}:stackset-target/\${StackSetTarget}	
type	arn:\${Partition}:cloudformation:\${Region}: \${Account}:type/resource/\${Type}	

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 [Available global condition 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
<code>cloudformation:ChangeSetControl</code>	Filters access by an AWS CloudFormation change set name. Use to control which change sets IAM users can execute or delete	String
<code>cloudformation:ImportType</code>	Filters access by the template resource types, such as <code>AWS::EC2::Instance</code> . Use to control which resource types IAM users can work with when they want to import a resource into a stack	String
<code>cloudformation:ResourceType</code>	Filters access by the template resource types, such as <code>AWS::EC2::Instance</code> . Use to control which resource types IAM users can work with when they create or update a stack	String
<code>cloudformation:RoleArn</code>	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
<code>cloudformation:StackPolicyURL</code>	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
<code>cloudformation:TargetRegions</code>	Filters access by stack set target region. Use to control which regions IAM users can use when they create or update stack sets	ArrayOfString
<code>cloudformation:TemplateURL</code>	Filters access by an Amazon S3 template URL. Use to control which templates IAM users can use when they create or update stacks	String

Actions, resources, and condition keys for Amazon CloudFront

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

References:

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

Topics

- [Actions defined by Amazon CloudFront \(p. 229\)](#)
- [Resource types defined by Amazon CloudFront \(p. 237\)](#)
- [Condition keys for Amazon CloudFront \(p. 238\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateAlias	Grants permission to associate an alias to a CloudFront distribution	Write	distribution* (p. 237)		
CreateCachePolicy	Grants permission to add a new cache policy to CloudFront	Write	cache-policy* (p. 237)		
CreateCloudFrontOriginAccessIdentity	Grants permission to create a new CloudFront origin access identity	Write	origin-access-identity* (p. 237)		
CreateDistribution	Grants permission to create a new web distribution	Write	distribution* (p. 237)		
CreateFieldLevelEncryptionConfiguration	Grants permission to create a new field-level encryption configuration	Write	field-level-encryption* (p. 237)		
CreateFieldLevelEncryptionProfile	Grants permission to create a field-level encryption profile	Write	field-level-encryption-profile* (p. 237)		
CreateFunction	Grants permission to create a CloudFront function	Write	function* (p. 237)		
CreateInvalidation	Grants permission to create a new invalidation batch request	Write	distribution* (p. 237)		
CreateKeyGroup	Grants permission to add a new key group to CloudFront	Write			
CreateMonitoring	Grants permission to enable additional CloudWatch metrics for the specified CloudFront distribution. The additional metrics incur an additional cost	Write			
CreateOriginRequestPolicy	Grants permission to add a new origin request policy to CloudFront	Write	origin-request-policy* (p. 237)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePublicKey	Grants permission to add a new public key to CloudFront	Write			
CreateRealtimeLogConfig	Grants permission to create a CloudFront log configuration	Write	realtime-log-config* (p. 237)		
CreateResponseHeaderPolicy	Grants permission to add a CloudFront response headers policy	Write	response-headers-policy* (p. 237)		
CreateStreamingDistribution	Grants permission to create a CloudFront streaming distribution	Write	streaming-distribution* (p. 237)		
CreateStreamingDistributionWithTags	Grants permission to create a CloudFront streaming distribution with tags	Write	streaming-distribution* (p. 237)		
				aws:RequestTag/\${TagKey} (p. 238)	aws:TagKeys (p. 238)
DeleteCachePolicy	Grants permission to delete a CloudFront cache policy	Write	cache-policy* (p. 237)		
DeleteCloudFrontOriginIdentity	Grants permission to delete a CloudFront origin identity	Write	origin-access-identity* (p. 237)		
DeleteDistribution	Grants permission to delete a CloudFront web distribution	Write	distribution* (p. 237)		
DeleteFieldLevelEncryption	Grants permission to delete a CloudFront field-level encryption configuration	Write	field-level-encryption* (p. 237)		
DeleteFieldLevelEncryptionProfile	Grants permission to delete a CloudFront field-level encryption profile	Write	field-level-encryption-profile* (p. 237)		
DeleteFunction	Grants permission to delete a CloudFront function	Write	function* (p. 237)		
DeleteKeyGroup	Grants permission to delete a CloudFront key group	Write			
DeleteMonitoring	Grants permission to disable CloudWatch metrics for the specified CloudFront distribution	Write			
DeleteOriginRequestPolicy	Grants permission to delete an CloudFront origin request policy	Write	origin-request-policy* (p. 237)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeletePublicKey	Grants permission to delete a public key from CloudFront	Write			
DeleteRealtimeLogConfig	Grants permission to delete a CloudFront log configuration	Write	realtime-log-config* (p. 237)		
DeleteResponseHeadersPolicy	Grants permission to delete a response headers policy	Write	response-headers-policy* (p. 237)		
DeleteStreamingDRTMPDistribution	Grants permission to delete an RTMP distribution	Write	streaming-distribution* (p. 237)		
DescribeFunction	Grants permission to get a CloudFront function summary	Read	function* (p. 237)		
GetCachePolicy	Grants permission to get the cache policy	Read	cache-policy* (p. 237)		
GetCachePolicyConfig	Grants permission to get the cache policy configuration	Read	cache-policy* (p. 237)		
GetCloudFrontOriginIdentity	Grants permission to get the information about a CloudFront origin access identity	Read	origin-access-identity* (p. 237)		
GetCloudFrontOriginConfiguration	Grants permission to get the configuration information about a Cloudfront origin access identity	Read	origin-access-identity* (p. 237)		
GetDistribution	Grants permission to get the information about a web distribution	Read	distribution* (p. 237)		
GetDistributionConfig	Grants permission to get the configuration information about a distribution	Read	distribution* (p. 237)		
GetFieldLevelEncryption	Grants permission to get the field-level encryption configuration information	Read	field-level-encryption* (p. 237)		
GetFieldLevelEncryptionConfig	Grants permission to get the field-level encryption configuration information	Read	field-level-encryption* (p. 237)		
GetFieldLevelEncryptionProfile	Grants permission to get the field-level encryption configuration information	Read	field-level-encryption-profile* (p. 237)		
GetFieldLevelEncryptionProfileConfig	Grants permission to get the field-level encryption profile configuration information	Read	field-level-encryption-profile* (p. 237)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetFunction	Grants permission to get a CloudFront function's code	Read	function* (p. 237)		
GetInvalidation	Grants permission to get the information about an invalidation	Read	distribution* (p. 237)		
GetKeyGroup	Grants permission to get a key group	Read			
GetKeyGroupConfig	Grants permission to get a key group configuration	Read			
GetMonitoringSubscription	Grants permission to get information about whether additional CloudWatch metrics are enabled for the specified CloudFront distribution	Read			
GetOriginRequestPolicy	Grants permission to get the origin request policy	Read	origin-request-policy* (p. 237)		
GetOriginRequestPolicyConfig	Grants permission to get the origin request policy configuration	Read	origin-request-policy* (p. 237)		
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* (p. 237)		
GetResponseHeadersPolicy	Grants permission to get the response headers policy	Read	response-headers-policy* (p. 237)		
GetResponseHeadersPolicyConfig	Grants permission to get the response headers policy configuration	Read	response-headers-policy* (p. 237)		
GetStreamingDistribution	Grants permission to get the information about an RTMP distribution	Read	streaming-distribution* (p. 237)		
GetStreamingDistributionConfig	Grants permission to get the configuration information about a streaming distribution	Read	streaming-distribution* (p. 237)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListCachePolicies	Grants permission to list all cache policies that have been created in CloudFront for this account	List			
ListCloudFrontOrigins	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* (p. 237)		
ListDistributions	Grants permission to list the distributions associated with your AWS account	List			
ListDistributionsByCachePolicy	Grants permission to list distribution IDs for distributions that have a cache behavior that's associated with the specified cache policy	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			
ListDistributionsByOriginRequestPolicy	Grants permission to list distribution IDs for distributions that have a cache behavior that's associated with the specified origin request policy	List			
ListDistributionsByRealtimeLogConfig	Grants permission to get a list of distribution IDs for distributions that have a cache behavior that's associated with the specified real-time log configuration	List			
ListDistributionsByResponseHeadersPolicy	Grants permission to list distribution IDs for distributions that have a cache behavior that's associated with the specified response headers policy	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDistributionsByDistributionId	Grants permission to list the distributions associated with your AWS account with given AWS WAF web ACL	List			
ListFieldLevelEncryptionAssociations	Grants permission to list 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* (p. 237)		
ListKeyGroups	Grants permission to list all key groups that have been created in CloudFront for this account	List			
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			
ListRealtimeLogConfigurations	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			
ListStreamingDistributions	Grants permission to list your RTMP distributions	List			
ListTagsForResource	Grants permission to list tags for a CloudFront resource	Read	distribution (p. 237)		
			streaming-distribution (p. 237)		
PublishFunction	Grants permission to publish a CloudFront function	Write	function* (p. 237)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to add tags to a CloudFront resource	Tagging	distribution (p. 237)		
			streaming-distribution (p. 237)		
				aws:RequestTag/\${TagKey} (p. 238)	aws:TagKeys (p. 238)
TestFunction	Grants permission to test a CloudFront function	Write	function* (p. 237)		
UntagResource	Grants permission to remove tags from a CloudFront resource	Tagging	distribution (p. 237)		
			streaming-distribution (p. 237)		
				aws:TagKeys (p. 238)	
UpdateCachePolicy	Grants permission to update a cache policy	Write	cache-policy* (p. 237)		
UpdateCloudFrontOriginAccessIdentity	Grants permission to set the configuration for a CloudFront origin access identity	Write	origin-access-identity* (p. 237)		
UpdateDistribution	Grants permission to update the configuration for a web distribution	Write	distribution* (p. 237)		
UpdateFieldLevelEncryption	Grants permission to update a field-level encryption configuration	Write	field-level-encryption* (p. 237)		
UpdateFieldLevelEncryptionProfile	Grants permission to update a field-level encryption profile	Write	field-level-encryption-profile* (p. 237)		
UpdateFunction	Grants permission to update a CloudFront function	Write	function* (p. 237)		
UpdateKeyGroup	Grants permission to update a key group	Write			
UpdateOriginRequestPolicy	Grants permission to update an origin request policy	Write	origin-request-policy* (p. 237)		
UpdatePublicKey	Grants permission to update public key information	Write			
UpdateRealtimeLogConfig	Grants permission to update a realtime log configuration	Write	realtime-log-config* (p. 237)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateResponseHeadersPolicy	Grants permission to update a response headers policy	Write	response-headers-policy* (p. 237)		
UpdateStreamingDistributionConfiguration	Grants permission to update the configuration for an RTMP distribution	Write	streaming-distribution* (p. 237)		

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 \(p. 229\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 238)
streaming-distribution	arn:\${Partition}:cloudfront::\${Account}:streaming-distribution/\${DistributionId}	aws:ResourceTag/\${TagKey} (p. 238)
origin-access-identity	arn:\${Partition}:cloudfront::\${Account}:origin-access-identity/\${Id}	
field-level-encryption	arn:\${Partition}:cloudfront::\${Account}:field-level-encryption/\${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}	
response-headers-policy	arn:\${Partition}:cloudfront::\${Account}:response-headers-policy/\${Id}	

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 [Available global condition keys](#).

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

Actions, resources, and condition keys for AWS CloudHSM

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

References:

- Learn how to [configure this service](#).
- View a list of the [API 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 \(p. 238\)](#)
- [Resource types defined by AWS CloudHSM \(p. 241\)](#)
- [Condition keys for AWS CloudHSM \(p. 241\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddTagsToResource	Adds or overwrites one or more tags for the specified AWS CloudHSM resource	Tagging			
CopyBackupToRegion	Creates a copy of a backup in the specified region	Write	backup* (p. 241)		
				aws:RequestTag/\${TagKey} (p. 241)	
				aws:TagKeys (p. 241)	
CreateCluster	Creates a new AWS CloudHSM cluster	Write	backup (p. 241)		
				aws:RequestTag/\${TagKey} (p. 241)	
				aws:TagKeys (p. 241)	
CreateHapg	Creates a high-availability partition group	Write			
CreateHsm	Creates a new hardware security module (HSM) in the specified AWS CloudHSM cluster	Write	cluster* (p. 241)		
CreateLunaClient	Creates an HSM client	Write			
DeleteBackup	Deletes the specified CloudHSM backup	Write	backup* (p. 241)		
DeleteCluster	Deletes the specified AWS CloudHSM cluster	Write	cluster* (p. 241)		
DeleteHapg	Deletes a high-availability partition group	Write			
DeleteHsm	Deletes the specified HSM	Write			
DeleteLunaClient	Deletes a client	Write			
DescribeBackups	Gets information about backups of AWS CloudHSM clusters	Read			
DescribeClusters	Gets information about AWS CloudHSM clusters	Read			
DescribeHapg	Retrieves information about a high-availability partition group	Read			
DescribeHsm	Retrieves information about an HSM. You can identify the HSM by its ARN or its serial number	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeLunaClient	Retrieves information about an HSM client	Read			
GetConfig	Gets the configuration files necessary to connect to all high availability partition groups the client is associated with	Read			
InitializeCluster	Claims an AWS CloudHSM cluster	Write	cluster* (p. 241)		
ListAvailableZone	Lists the Availability Zones that have available AWS CloudHSM capacity	List			
ListHapgs	Lists the high-availability partition groups for the account	List			
ListHsms	Retrieves the identifiers of all of the HSMs provisioned for the current customer	List			
ListLunaClients	Lists all of the clients	List			
ListTags	Gets a list of tags for the specified AWS CloudHSM cluster	Read	backup (p. 241) cluster (p. 241)		
ListTagsForResource	Returns a list of all tags for the specified AWS CloudHSM resource	Read			
ModifyBackupAttribute	Modifies attributes for AWS CloudHSM backup	Write	backup* (p. 241)		
ModifyCluster	Modifies AWS CloudHSM cluster.	Write	cluster* (p. 241)		
ModifyHapg	Modifies an existing high-availability partition group	Write			
ModifyHsm	Modifies an HSM	Write			
ModifyLunaClient	Modifies the certificate used by the client	Write			
RemoveTagsFromResource	Removes one or more tags from the specified AWS CloudHSM resource	Tagging			
RestoreBackup	Restores the specified CloudHSM backup	Write	backup* (p. 241)		
TagResource	Adds or overwrites one or more tags for the specified AWS CloudHSM cluster	Tagging	backup (p. 241) cluster (p. 241)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 241) aws:TagKeys (p. 241)	
UntagResource	Removes the specified tag or tags from the specified AWS CloudHSM cluster	Tagging	backup (p. 241)		
			cluster (p. 241)		
			aws:TagKeys (p. 241)		

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 \(p. 238\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
backup	arn:\${Partition}:clouddhsm: \${Region}:\${Account}:backup/ \${CloudHsmBackupInstanceName}	aws:ResourceTag/ \${TagKey} (p. 241)
cluster	arn:\${Partition}:clouddhsm: \${Region}:\${Account}:cluster/ \${CloudHsmClusterInstanceName}	aws:ResourceTag/ \${TagKey} (p. 241)

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 [Available global condition 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	String

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 \(p. 242\)](#)
- [Resource types defined by Amazon CloudSearch \(p. 244\)](#)
- [Condition keys for Amazon CloudSearch \(p. 245\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 245)		
BuildSuggesters	Indexes the search suggestions.	Write	domain* (p. 245)		
CreateDomain	Creates a new search domain.	Write	domain* (p. 245)		
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* (p. 245)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DefineExpression	Configures an Expression for the search domain.	Write	domain* (p. 245)		
DefineIndexField	Configures an IndexField for the search domain.	Write	domain* (p. 245)		
DefineSuggester	Configures a suggester for a domain.	Write	domain* (p. 245)		
DeleteAnalysisScheme	Deletes an analysis scheme.	Write	domain* (p. 245)		
DeleteDomain	Permanently deletes a search domain and all of its data.	Write	domain* (p. 245)		
DeleteExpression	Removes an Expression from the search domain.	Write	domain* (p. 245)		
DeleteIndexField	Removes an IndexField from the search domain.	Write	domain* (p. 245)		
DeleteSuggester	Deletes a suggester.	Write	domain* (p. 245)		
DescribeAnalysisSchemes	Gets the analysis schemes configured for a domain.	Read	domain* (p. 245)		
DescribeAvailabilityConfigurations	Gets the availability options configured for a domain.	Read	domain* (p. 245)		
DescribeDomainEndpointConfigurations	Gets the domain endpoint options configured for a domain.	Read	domain* (p. 245)		
DescribeDomains	Gets information about the search domains owned by this account.	List	domain* (p. 245)		
DescribeExpressions	Gets the expressions configured for the search domain.	Read	domain* (p. 245)		
DescribeIndexFields	Gets information about the index fields configured for the search domain.	Read	domain* (p. 245)		
DescribeScalingParameters	Gets the scaling parameters configured for a domain.	Read	domain* (p. 245)		
DescribeServiceAccessPolicies	Gets information about the access policies that control access to the domain's document and search endpoints.	Read	domain* (p. 245)		
DescribeSuggesters	Gets the suggesters configured for a domain.	Read	domain* (p. 245)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
IndexDocuments	Tells the search domain to start indexing its documents using the latest indexing options.	Write	domain* (p. 245)		
ListDomainNames	Lists all search domains owned by an account.	List	domain* (p. 245)		
ListTags	Displays all of the resource tags for an Amazon CloudSearch domain.	Read	domain* (p. 245)		
RemoveTags	Removes the specified resource tags from an Amazon ES domain.	Tagging	domain* (p. 245)		
UpdateAvailabilityOptions	Configures the availability options for a domain.	Write	domain* (p. 245)		
UpdateDomainEndpointOptions	Configures the domain endpoint options for a domain.	Write	domain* (p. 245)		
UpdateScalingParameters	Configures scaling parameters for a domain.	Write	domain* (p. 245)		
UpdateServiceAccessControlPolicies	Configures the access rules that control access to the domain's document and search endpoints.	Permissions management	domain* (p. 245)		
document [permission only]	Allows access to the document service operations.	Write	domain (p. 245)		
search [permission only]	Allows access to the search operations.	Read	domain (p. 245)		
suggest [permission only]	Allows access to the suggest operations.	Read	domain (p. 245)		

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 \(p. 242\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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 [Available keys for conditions](#).

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 \(p. 245\)](#)
- [Resource types defined by AWS CloudShell \(p. 246\)](#)
- [Condition keys for AWS CloudShell \(p. 247\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateEnvironment [permission only]	Grants permissions to create a CloudShell environment	Write			
CreateSession [permission only]	Grants permissions to connect to a CloudShell environment from the AWS Management Console	Write	Environment* (p. 247)		
DeleteEnvironment [permission only]	Grants permission to delete a CloudShell environment	Write	Environment* (p. 247)		
GetEnvironmentStatus [permission only]	Grants permission to read a CloudShell environment status	Read	Environment* (p. 247)		
GetFileDownloadUrls [permission only]	Grants permissions to download files from a CloudShell environment	Write	Environment* (p. 247)		
GetFileUploadUrls [permission only]	Grants permissions to upload files to a CloudShell environment	Write	Environment* (p. 247)		
PutCredentials [permission only]	Grants permissions to forward console credentials to the environment	Write	Environment* (p. 247)		
StartEnvironment [permission only]	Grants permission to start a stopped CloudShell environment	Write	Environment* (p. 247)		
StopEnvironment [permission only]	Grants permission to stop a running CloudShell environment	Write	Environment* (p. 247)		

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 \(p. 245\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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

CloudShell 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 [Available keys for conditions](#).

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 \(p. 247\)](#)
- [Resource types defined by AWS CloudTrail \(p. 250\)](#)
- [Condition keys for AWS CloudTrail \(p. 250\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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, up to a limit of 10	Tagging	eventdatastore (p. 250)		
			trail (p. 250)		
CancelQuery	Grants permission to cancel a running query	Write			
CreateEventDataStore	Grants permission to create an event data store	Write	eventdatastore* (p. 250)		
				aws:RequestTag/\${TagKey} (p. 250)	
				aws:TagKeys (p. 250)	
CreateTrail	Grants permission to create a trail that specifies the settings for delivery of log data to an Amazon S3 bucket	Write	trail* (p. 250)		s3:PutObject
DeleteEventDataStore	Grants permission to delete an event data store	Write	eventdatastore* (p. 250)		
DeleteTrail	Grants permission to delete a trail	Write	trail* (p. 250)		
DescribeQuery	Grants permission to list details for the query	Read			
DescribeTrails	Grants permission to list settings for the trails associated with the current region for your account	Read			
GetEventDataStore	Grants permission to list settings for the event data store	Read			
GetEventSelector	Grants permission to list settings for event selectors configured for a trail	Read	trail* (p. 250)		
GetInsightSelector	Grants permission to list CloudTrail Insights selectors that are configured for a trail	Read	trail* (p. 250)		
GetQueryResults	Grants permission to fetch results of a complete query	Read			
GetTrail	Grants permission to list settings for the trail	Read			
GetTrailStatus	Grants permission to retrieve a JSON-formatted list of information about the specified trail	Read	trail* (p. 250)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListEventDataStores	Grants permission to list event data stores associated with the current region for your account	List			
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			
ListTags	Grants permission to list the tags for trails or event data stores in the current region	Read	eventdatastore (p. 250)		
			trail (p. 250)		
ListTrails	Grants permission to list trails associated with the current region for your account	List			
LookupEvents	Grants permission to look up API activity events captured by CloudTrail that create, update, or delete resources in your account	Read			
PutEventSelectors	Grants permission to create and update event selectors for a trail	Write	trail* (p. 250)		
PutInsightSelectors	Grants permission to create and update CloudTrail Insights selectors for a trail	Write	trail* (p. 250)		
RemoveTags	Grants permission to remove tags from a trail	Tagging	eventdatastore (p. 250)		
			trail (p. 250)		
RestoreEventDataStores	Grants permission to restore an event data store	Write	eventdatastore* (p. 250)		
StartLogging	Grants permission to start the recording of AWS API calls and log file delivery for a trail	Write	trail* (p. 250)		
StartQuery	Grants permission to start a new query on a specified event data store	Write			
StopLogging	Grants permission to stop the recording of AWS API calls and log file delivery for a trail	Write	trail* (p. 250)		
UpdateEventDataStores	Grants permission to update an event data store	Write	eventdatastore* (p. 250)		

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* (p. 250)		

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 \(p. 247\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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 [Granting Custom Permissions](#) in the *AWS CloudTrail User Guide*.

Resource types	ARN	Condition keys
trail	arn:\${Partition}:cloudtrail:\${Region}: \${Account}:trail/\${TrailName}	
eventdatastore	arn:\${Partition}:cloudtrail: \${Region}: \${Account}:eventdatastore/ \${EventDatastoreId}	aws:ResourceTag/\${TagKey} (p. 250)

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 [Available global condition keys](#).

Condition keys	Description	Type
aws:RequestTag/\${TagKey}	Filters access by value associated with the resource	String
aws:ResourceTag/\${TagKey}	Filters access by value associated with the resource	String
aws:TagKeys	Filters access by value associated with the resource	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 \(p. 251\)](#)
- [Resource types defined by Amazon CloudWatch \(p. 255\)](#)
- [Condition keys for Amazon CloudWatch \(p. 255\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAlarms	Grants permission to delete a collection of alarms	Write	alarm* (p. 255)		
DeleteAnomalyDetector	Grants permission to delete the specified anomaly detection model from your account	Write			
DeleteDashboard	Grants permission to delete all CloudWatch dashboards that you specify	Write	dashboard* (p. 255)		
DeleteInsightRule	Grants permission to delete a collection of insight rules	Write	insight-rule* (p. 255)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteMetricStream	Grants permission to delete the CloudWatch metric stream that you specify	Write	metric-stream* (p. 255)		
DescribeAlarmHistory	Grants permission to retrieve the history for the specified alarm	Read	alarm* (p. 255)		
DescribeAlarms	Grants permission to describe all alarms, currently owned by the user's account	Read	alarm* (p. 255)		
DescribeAlarmsForMetrics	Grants permission to describe all alarms configured on the specified metric, currently owned by the user's account	Read			
DescribeAnomalyDetector	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* (p. 255)		
DisableInsightRules	Grants permission to disable a collection of insight rules	Write	insight-rule* (p. 255)		
EnableAlarmActions	Grants permission to enable actions for a collection of alarms	Write	alarm* (p. 255)		
EnableInsightRules	Grants permission to enable a collection of insight rules	Write	insight-rule* (p. 255)		
GetDashboard	Grants permission to display the details of the CloudWatch dashboard you specify	Read	dashboard* (p. 255)		
GetInsightRuleReport	Grants permission to return the top-N report of unique contributors over a time range for a given insight rule	Read	insight-rule* (p. 255)		
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* (p. 255)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetMetricWidgetSnapshots	Grants permission to retrieve snapshots of metric widgets	Read			
ListDashboards	Grants permission to return a list of all CloudWatch dashboards in your account	List			
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			
ListTagsForResource	Grants permission to list tags for an Amazon CloudWatch resource	List	alarm (p. 255)		
	SCENARIO: CloudWatch-Alarm		alarm* (p. 255)		
	SCENARIO: CloudWatch-InsightRule		insight-rule* (p. 255)		
PutAnomalyDetectionModel	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* (p. 255)		
				aws:RequestTag/\${TagKey} (p. 255)	
				aws:TagKeys (p. 255)	
				cloudwatch:AlarmActions (p. 255)	
PutDashboard	Grants permission to create a CloudWatch dashboard, or update an existing dashboard if it already exists	Write	dashboard* (p. 255)		
PutInsightRule	Grants permission to create a new insight rule or replace an existing insight rule	Write	insight-rule* (p. 255)		
				aws:RequestTag/\${TagKey} (p. 255)	
				aws:TagKeys (p. 255)	
				cloudwatch:requestInsightRuleLogGroup (p. 255)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions	
PutMetricAlarm	Grants permission to create or update an alarm and associates it with the specified Amazon CloudWatch metric	Write	alarm* (p. 255)			
				aws:RequestTag/\${TagKey} (p. 255)		
				aws:TagKeys (p. 255)		
PutMetricData	Grants permission to publish metric data points to Amazon CloudWatch	Write		cloudwatch:namespace (p. 255)		
PutMetricStream	Grants permission to create a CloudWatch metric stream, or update an existing metric stream if it already exists	Write	metric-stream* (p. 255)			
				aws:RequestTag/\${TagKey} (p. 255)		
				aws:TagKeys (p. 255)		
SetAlarmState	Grants permission to temporarily set the state of an alarm for testing purposes	Write	alarm* (p. 255)			
StartMetricStream	Grants permission to start all CloudWatch metric streams that you specify	Write	metric-stream* (p. 255)			
StopMetricStream	Grants permission to stop all CloudWatch metric streams that you specify	Write	metric-stream* (p. 255)			
TagResource	Grants permission to add tags to an Amazon CloudWatch resource	Tagging	alarm (p. 255)			
			insight-rule (p. 255)			
				aws:TagKeys (p. 255)		
				aws:RequestTag/\${TagKey} (p. 255)		
SCENARIO: CloudWatch-Alarm			alarm* (p. 255)			
	SCENARIO: CloudWatch-InsightRule	Tagging	insight-rule* (p. 255)			
UntagResource	Grants permission to remove a tag from an Amazon CloudWatch resource		alarm (p. 255)			
			insight-rule (p. 255)			
				aws:TagKeys (p. 255)		
SCENARIO: CloudWatch-Alarm		Tagging	alarm* (p. 255)			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	SCENARIO: CloudWatch- InsightRule		insight- rule* (p. 255)		

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 \(p. 251\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
alarm	<code>arn:\${Partition}:cloudwatch:\${Region}: \${Account}:alarm:\${AlarmName}</code>	aws:ResourceTag/ \${TagKey} (p. 255)
dashboard	<code>arn:\${Partition}:cloudwatch:: \${Account}:dashboard/\${DashboardName}</code>	
insight-rule	<code>arn:\${Partition}:cloudwatch:\${Region}: \${Account}:insight-rule/\${InsightRuleName}</code>	aws:ResourceTag/ \${TagKey} (p. 255)
metric-stream	<code>arn:\${Partition}:cloudwatch:\${Region}: \${Account}:metric-stream/\${MetricStreamName}</code>	aws:ResourceTag/ \${TagKey} (p. 255)

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 [Available global condition 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:namespacevalues	Filters actions based on the presence of optional namespace	String

Condition keys	Description	Type
<code>cloudwatch:requestInInsightRuleLogGroups</code>	Filters actions based on the Log Groups specified in an CloudWatch Application Insights rule .	ArrayOfString

Actions, resources, and condition keys for CloudWatch Application Insights

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 CloudWatch Application Insights \(p. 256\)](#)
- [Resource types defined by CloudWatch Application Insights \(p. 258\)](#)
- [Condition keys for CloudWatch Application Insights \(p. 258\)](#)

Actions defined by 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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 from a resource group	Write			
CreateComponent	Grants permission to create a component from a group of resources	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLogPattern	Grants permission to create log pattern	Write			
DeleteApplication	Grants permission to delete an application	Write			
DeleteComponent	Grants permission to delete a component	Write			
DeleteLogPattern	Grants permission to delete a log pattern	Write			
DescribeApplication	Grants permission to describe an application	Read			
DescribeComponent	Grants permission to describe a component	Read			
DescribeComponentConfiguration	Grants permission to describe a component configuration	Read			
DescribeComponentRecommendation	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			
DescribeProblemObservation	Grants permission to describe the observation in a problem	Read			
ListApplications	Grants permission to list all applications	List			
ListComponent	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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to list tags for the resource	Read			
TagResource	Grants permission to tag a resource	Tagging			
UntagResource	Grants permission to untag a resource	Tagging			
UpdateApplication	Grants permission to update an application	Write			
UpdateComponent	Grants permission to update a component	Write			
UpdateComponentType	Grants permission to update a component type configuration	Write			
UpdateLogPattern	Grants permission to update a log pattern	Write			

Resource types defined by CloudWatch Application Insights

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

Condition keys for CloudWatch Application Insights

CloudWatch Application Insights 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 [Available keys for conditions](#).

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 \(p. 259\)](#)
- [Resource types defined by Amazon CloudWatch Evidently \(p. 261\)](#)
- [Condition keys for Amazon CloudWatch Evidently \(p. 261\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 261)		
CreateExperiment	Grants permission to create an experiment	Write		aws:RequestTag/\${TagKey} (p. 262) aws:TagKeys (p. 262)	
CreateFeature	Grants permission to create a feature	Write		aws:RequestTag/\${TagKey} (p. 262) aws:TagKeys (p. 262)	
CreateLaunch	Grants permission to create a launch	Write		aws:RequestTag/\${TagKey} (p. 262) aws:TagKeys (p. 262)	
CreateProject	Grants permission to create a project	Write		aws:RequestTag/\${TagKey} (p. 262) aws:TagKeys (p. 262)	
DeleteExperiment	Grants permission to delete an experiment	Write	Experiment* (p. 261)		
DeleteFeature	Grants permission to delete a feature	Write	Feature* (p. 261)		
DeleteLaunch	Grants permission to delete a launch	Write	Launch* (p. 261)		
DeleteProject	Grants permission to delete a project	Write	Project* (p. 261)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EvaluateFeature	Grants permission to send an evaluate feature request	Write	Feature* (p. 261)		
GetExperiment	Grants permission to get experiment details	Read	Experiment* (p. 261)		
GetExperimentResult	Grants permission to get experiment result	Read	Experiment* (p. 261)		
GetFeature	Grants permission to get feature details	Read	Feature* (p. 261)		
GetLaunch	Grants permission to get launch details	Read	Launch* (p. 261)		
GetProject	Grants permission to get project details	Read	Project* (p. 261)		
ListExperiments	Grants permission to list experiments	Read			
ListFeatures	Grants permission to list features	Read			
ListLaunches	Grants permission to list launches	Read			
ListProjects	Grants permission to list projects	Read			
ListTagsForResource	Grants permission to list tags for resources	Read			
PutProjectEvents	Grants permission to send performance events	Write	Project* (p. 261)		
StartExperiment	Grants permission to start an experiment	Write	Experiment* (p. 261)		
StartLaunch	Grants permission to start a launch	Write	Launch* (p. 261)		
StopExperiment	Grants permission to stop an experiment	Write	Experiment* (p. 261)		
StopLaunch	Grants permission to stop a launch	Write	Launch* (p. 261)		
TagResource	Grants permission to tag resources	Tagging		aws:RequestTag/\${TagKey} (p. 262) aws:TagKeys (p. 262)	
UntagResource	Grants permission to untag resources	Tagging		aws:RequestTag/\${TagKey} (p. 262) aws:TagKeys (p. 262)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateExperiment	Grants permission to update experiment	Write	Experiment* (p. 261)		
UpdateFeature	Grants permission to update feature	Write	Feature* (p. 261)		
UpdateLaunch	Grants permission to update a launch	Write	Launch* (p. 261)		
UpdateProject	Grants permission to update project	Write	Project* (p. 261)		
UpdateProjectDataDelivery	Grants permission to update project data delivery	Write	Project* (p. 261)		

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 \(p. 259\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
Project	<code>arn:\${Partition}:evidently:\${Region}: \${OwnerAccountId}:project/\${ProjectName}</code>	aws:ResourceTag/\${TagKey} (p. 262)
Feature	<code>arn:\${Partition}:evidently:\${Region}: \${OwnerAccountId}:project/\${ProjectName}/feature/\${FeatureName}</code>	aws:ResourceTag/\${TagKey} (p. 262)
Experiment	<code>arn:\${Partition}:evidently:\${Region}: \${OwnerAccountId}:project/\${ProjectName}/experiment/\${ExperimentName}</code>	aws:ResourceTag/\${TagKey} (p. 262)
Launch	<code>arn:\${Partition}:evidently:\${Region}: \${OwnerAccountId}:project/\${ProjectName}/launch/\${LaunchName}</code>	aws:ResourceTag/\${TagKey} (p. 262)

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 [Available global condition 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 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 \(p. 262\)](#)
- [Resource types defined by Amazon CloudWatch Logs \(p. 266\)](#)
- [Condition keys for Amazon CloudWatch Logs \(p. 267\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 permissions to associate the specified AWS Key	Write	log-group* (p. 267)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Management Service (AWS KMS) customer master key (CMK) with the specified log group				
CancelExportTask	Grants permissions to cancel an export task if it is in PENDING or RUNNING state	Write			
CreateExportTask	Grants permissions to create an ExportTask which allows you to efficiently export data from a Log Group to your Amazon S3 bucket	Write	log-group* (p. 267)		
CreateLogDelivery [permission only]	Grants permissions to create the log delivery	Write			
CreateLogGroup	Grants permissions to create a new log group with the specified name	Write	log-group* (p. 267)		
CreateLogStream	Grants permissions to create a new log stream with the specified name	Write	log-group* (p. 267)		
DeleteDestination	Grants permissions to delete the destination with the specified name	Write			
DeleteLogDelivery [permission only]	Grants permissions to delete the log delivery information for specified log delivery	Write			
DeleteLogGroup	Grants permissions to delete the log group with the specified name	Write	log-group* (p. 267)		
DeleteLogStream	Grants permissions to delete a log stream	Write	log-stream* (p. 267)		
DeleteMetricFilter	Grants permissions to delete a metric filter associated with the specified log group	Write	log-group* (p. 267)		
DeleteQueryDefinition	Grants permissions to delete a saved CloudWatch Logs Insights query definition	Write			
DeleteResourcePolicy	Grants permissions to delete a resource policy from this account	Permissions management			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteRetentionPolicy	Grants permissions to delete the retention policy of the specified log group	Write	log-group* (p. 267)		
DeleteSubscriptionFilter	Grants permissions to delete a subscription filter associated with the specified log group	Write	log-group* (p. 267)		
DescribeDestinations	Grants permissions to return all the destinations that are associated with the AWS account making the request	List			
DescribeExportTasks	Grants permissions to return all the export tasks that are associated with the AWS account making the request	List			
DescribeLogGroups	Grants permissions to return all the log groups that are associated with the AWS account making the request	List	log-group* (p. 267)		
DescribeLogStreams	Grants permissions to return all the log streams that are associated with the specified log group	List	log-group* (p. 267)		
DescribeMetricFilters	Grants permissions to return all the metrics filters associated with the specified log group	List	log-group* (p. 267)		
DescribeQueries	Grants permissions to return a list of CloudWatch Logs Insights queries that are scheduled, executing, or have been executed recently in this account	List			
DescribeQueryDefinitions	Grants permissions to return a paginated list of your saved CloudWatch Logs Insights query definitions	List			
DescribeResourcePolicies	Grants permissions to return all the resource policies in this account	List			
DescribeSubscriptionFilters	Grants permissions to return all the subscription filters associated with the specified log group	List	log-group* (p. 267)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateKmsKey	Grants permissions to disassociate the associated AWS Key Management Service (AWS KMS) customer master key (CMK) from the specified log group	Write	log-group* (p. 267)		
FilterLogEvents	Grants permissions to retrieve log events, optionally filtered by a filter pattern from the specified log group	Read	log-group* (p. 267)		
GetLogDelivery [permission only]	Grants permissions to get the log delivery information for specified log delivery	Read			
GetLogEvents	Grants permissions to retrieve log events from the specified log stream	Read	log-stream* (p. 267)		
GetLogGroupFields	Grants permissions 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* (p. 267)		
GetLogRecord	Grants permissions to retrieve all the fields and values of a single log event	Read			
GetQueryResults	Grants permissions to return the results from the specified query	Read			
ListLogDeliveries [permission only]	Grants permissions to list all the log deliveries for specified account and/or log source	List			
ListTagsLogGroup	Grants permissions to list the tags for the specified log group	List	log-group* (p. 267)		
PutDestination	Grants permissions to create or update a Destination	Write			iam:PassRole
PutDestinationPolicy	Grants permissions to create or update an access policy associated with an existing Destination	Write			
PutLogEvents	Grants permissions to upload a batch of log events to the specified log stream	Write	log-stream* (p. 267)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutMetricFilter	Grants permissions to create or update a metric filter and associates it with the specified log group	Write	log-group* (p. 267)		
PutQueryDefinition	Grants permissions to create or update a query definition	Write			
PutResourcePolicy	Grants permissions to create or update a resource policy allowing other AWS services to put log events to this account	Permissions management			
PutRetentionPolicy	Grants permissions to set the retention of the specified log group	Write	log-group* (p. 267)		
PutSubscriptionFilter	Grants permissions to create or update a subscription filter and associates it with the specified log group	Write	log-group* (p. 267)	destination (p. 267)	iam:PassRole
StartQuery	Grants permissions to schedules a query of a log group using CloudWatch Logs Insights	Read	log-group* (p. 267)		
StopQuery	Grants permissions to stop a CloudWatch Logs Insights query that is in progress	Read			
TagLogGroup	Grants permissions to add or update the specified tags for the specified log group	Tagging	log-group* (p. 267)		
TestMetricFilter	Grants permissions to test the filter pattern of a metric filter against a sample of log event messages	Read			
UntagLogGroup	Grants permissions to remove the specified tags from the specified log group	Tagging	log-group* (p. 267)		
UpdateLogDelivery [permission only]	Grants permissions to update the log delivery information for specified log delivery	Write			

Resource types defined by Amazon CloudWatch Logs

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the [Actions table](#) (p. 262) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you

can include in a policy. These keys are displayed in the last column of the 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} (p. 267)
log-stream	arn:\${Partition}:logs:\${Region}: \${Account}:log-group:\${LogGroupName}:log-stream:\${LogStreamName}	
destination	arn:\${Partition}:logs:\${Region}: \${Account}:destination:\${DestinationName}	

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 [Available global condition keys](#).

Condition keys	Description	Type
aws:ResourceTag/\${TagKey}	Filters access based on the tags associated with the resource	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 \(p. 267\)](#)
- [Resource types defined by AWS CloudWatch RUM \(p. 269\)](#)
- [Condition keys for AWS CloudWatch RUM \(p. 269\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAppMonitor	Grants permission to create appMonitor metadata	Write	AppMonitorResource* (p. 269)	iam:CreateServiceLinkedRole	iam:GetRole
				aws:RequestTag/\${TagKey} (p. 269)	
				aws:TagKeys (p. 269)	
DeleteAppMonitor	Grants permission to delete appMonitor metadata	Write	AppMonitorResource* (p. 269)		
GetAppMonitor	Grants permission to get appMonitor metadata	Read	AppMonitorResource* (p. 269)		
GetAppMonitorData	Grants permission to get appMonitor data	Read	AppMonitorResource* (p. 269)		
ListAppMonitors	Grants permission to list appMonitors metadata	List			
ListTagsForResource	Grants permission to list tags for resources	Read			
PutRumEvents	Grants permission to put RUM events for appmonitor	Write	AppMonitorResource* (p. 269)		
TagResource	Grants permission to tag resources	Tagging		aws:RequestTag/\${TagKey} (p. 269)	
				aws:TagKeys (p. 269)	
UntagResource	Grants permission to untag resources	Tagging		aws:RequestTag/\${TagKey} (p. 269)	
				aws:TagKeys (p. 269)	
UpdateAppMonitor	Grants permission to update appmonitor metadata	Write	AppMonitorResource* (p. 269)	iam:CreateServiceLinkedRole	iam:GetRole

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 \(p. 267\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
AppMonitorResource	<code>arn:\${Partition}:rum:\${Region}: \${Account}:appmonitor/\${Name}</code>	<code>aws:ResourceTag/ \${TagKey}</code> (p. 269)

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/ \${TagKey}</code>	Filters access by the tags that are passed the request on behalf of the IAM principal	String
<code>aws:ResourceTag/ \${TagKey}</code>	Filters access by the tags associated with the resource that make the request on behalf of the IAM principal	String
<code>aws:TagKeys</code>	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 \(p. 270\)](#)
- [Resource types defined by Amazon CloudWatch Synthetics \(p. 271\)](#)
- [Condition keys for Amazon CloudWatch Synthetics \(p. 271\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCanary	Grants permission to create a canary	Write		aws:RequestTag/\${TagKey} (p. 271) aws:TagKeys (p. 271)	
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* (p. 271)		
DescribeCanaries	Grants permission to list information of all canaries	Read		synthetics:Names (p. 272)	
DescribeCanariesInformation	Grants permission to list information about the last test run associated with all canaries	Read		synthetics:Names (p. 272)	
DescribeRuntimeInformation	Grants permission to list information about Synthetics canary runtime versions	Read			
GetCanary	Grants permission to get a canary details	Read	canary* (p. 271)		
GetCanaryRuns	Grants permission to list information about all the test runs associated with a canary	Read	canary* (p. 271)		
ListTagsForResource	Grants permission to list all tags and values associated with a canary	Read	canary (p. 271)		
StartCanary	Grants permission to start a canary, so that Amazon	Write	canary* (p. 271)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	CloudWatch Synthetics starts monitoring a website				
StopCanary	Grants permission to stop a canary	Write	canary* (p. 271)		
TagResource	Grants permission to add one or more tags to a canary	Tagging	canary (p. 271)		
				aws:RequestTag/\${TagKey} (p. 271) aws:TagKeys (p. 271)	
UntagResource	Grants permission to remove one or more tags from a canary	Tagging	canary (p. 271)		
				aws:TagKeys (p. 271)	
UpdateCanary	Grants permission to update a canary	Write	canary* (p. 271)		

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](#) (p. 270) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 271)

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 [Available global condition 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

Condition keys	Description	Type
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 \(p. 272\)](#)
- [Resource types defined by AWS CodeArtifact \(p. 275\)](#)
- [Condition keys for AWS CodeArtifact \(p. 276\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateExternalRepository	Grants permission to add an external connection to a repository	Write	repository* (p. 275)		
AssociateWithDownstreamRepository	Grants permission to associate an existing repository as an upstream repository to another repository	Write	repository* (p. 275)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CopyPackageVersion	Grants permission to copy package versions from one repository to another repository in the same domain	Write	package* (p. 275)		
			repository* (p. 275)		
CreateDomain	Grants permission to create a new domain	Write		aws:RequestTag/\${TagKey} (p. 276) aws:TagKeys (p. 276)	
CreateRepository	Grants permission to create a new repository	Write		aws:RequestTag/\${TagKey} (p. 276) aws:TagKeys (p. 276)	
DeleteDomain	Grants permission to delete a domain	Write	domain* (p. 275)		
DeleteDomainPermissions	Grants permission to delete the resource policy set on a domain	Permissions management	domain* (p. 275)		
DeletePackageVersions	Grants permission to delete package versions	Write	package* (p. 275)		
DeleteRepository	Grants permission to delete a repository	Write	repository* (p. 275)		
DeleteRepositoryPermissions	Grants permission to delete the resource policy set on a repository	Permissions management	repository* (p. 275)		
DescribeDomain	Grants permission to return information about a domain	Read	domain* (p. 275)		
DescribePackageVersion	Grants permission to return information about a package version	Read	package* (p. 275)		
DescribeRepository	Grants permission to return detailed information about a repository	Read	repository* (p. 275)		
DisassociateExternalAssociations	Grants permission to disassociate external connection from a repository	Write	repository* (p. 275)		
DisposePackageVersions	Grants permission to set the status of package versions to Disposed and delete their assets	Write	package* (p. 275)		
GetAuthorizationToken	Grants permission to generate a temporary authentication token for accessing repositories in a domain	Read	domain* (p. 275)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDomainPermissionsPreview	Grants permission to return a domain's resource policy	Read	domain* (p. 275)		
GetPackageVersionAssets	Grants permission to return an asset (or file) that is part of a package version	Read	package* (p. 275)		
GetPackageVersionReadme	Grants permission to return a package version's readme file	Read	package* (p. 275)		
GetRepositoryEndpoint	Grants permission to return an endpoint for a repository	Read	repository* (p. 275)		
GetRepositoryPermissionsPreview	Grants permission to return a repository's resource policy	Read	repository* (p. 275)		
ListDomains	Grants permission to list the domains in the current user's AWS account	List			
ListPackageVersionAssets	Grants permission to list a package version's assets	List	package* (p. 275)		
ListPackageVersionDependencies	Grants permission to list the direct dependencies of a package version	List	package* (p. 275)		
ListPackageVersions	Grants permission to list a package's versions	List	package* (p. 275)		
ListPackages	Grants permission to list the packages in a repository	List	repository* (p. 275)		
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* (p. 275)		
ListTagsForResource	Grants permission to list tags for a CodeArtifact resource	List	domain (p. 275) repository (p. 275)		
PublishPackageVersionAssets	Grants permission to publish assets and metadata to a repository endpoint	Write	package* (p. 275)		
PutDomainPermissionsPreview	Grants permission to attach a resource policy to a domain	Write	domain* (p. 275)		
PutPackageMetadata	Grants permission to add, modify or remove package metadata using a repository endpoint	Write	package* (p. 275)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutRepositoryPermissionPolicy	Grants permission to attach a repository policy to a repository	Write	repository* (p. 275)		
ReadFromRepository	Grants permission to return package assets and metadata from a repository endpoint	Read	repository* (p. 275)		
TagResource	Grants permission to tag a CodeArtifact resource	Tagging	domain (p. 275)		
			repository (p. 275)		
			aws:RequestTag/\${TagKey} (p. 276)		
UntagResource	Grants permission to remove a tag from a CodeArtifact resource	Tagging	aws:TagKeys (p. 276)		
			domain (p. 275)		
			repository (p. 275)		
UpdatePackageVersionStatus	Grants permission to modify the status of one or more versions of a package	Write	package* (p. 275)		
UpdateRepository	Grants permission to modify the properties of a repository	Write	repository* (p. 275)		

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 \(p. 272\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
domain	<code>arn:\${Partition}:codeartifact:\${Region}: \${Account}:domain/\${DomainName}</code>	aws:ResourceTag/\${TagKey} (p. 276)
repository	<code>arn:\${Partition}:codeartifact:\${Region}: \${Account}:repository/\${DomainName}/ \${RepositoryName}</code>	aws:ResourceTag/\${TagKey} (p. 276)
package	<code>arn:\${Partition}:codeartifact:\${Region}: \${Account}:package/\${DomainName}/ \${RepositoryName}/\${PackageFormat}/ \${PackageNameSpace}/\${PackageName}</code>	

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters actions based on the presence of tag key-value pairs in the request	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters actions based on tag key-value pairs attached to the resource	String
<code>aws:TagKeys</code>	Filters actions based on 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 \(p. 276\)](#)
- [Resource types defined by AWS CodeBuild \(p. 281\)](#)
- [Condition keys for AWS CodeBuild \(p. 282\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 282)		
BatchGetBuildBatches	Grants permission to get information about one or more build batches	Read	project* (p. 282)		
BatchGetBuilds	Grants permission to get information about one or more builds	Read	project* (p. 282)		
BatchGetProjects	Grants permission to get information about one or more build projects	Read	project* (p. 282)		
BatchGetReportGroups	Grants permission to return an array of ReportGroup objects that are specified by the input reportGroupArns parameter	Read	report-group* (p. 282)		
BatchGetReports	Grants permission to return an array of the Report objects specified by the input reportArns parameter	Read	report-group* (p. 282)		
BatchPutCodeCoverage [permission only]	Grants permission to add or update information about a report	Write	report-group* (p. 282)		
BatchPutTestCaseResults [permission only]	Grants permission to add or update information about a report	Write	report-group* (p. 282)		
CreateProject	Grants permission to create a build project	Write	project* (p. 282)		
				aws:RequestTag/\${TagKey} (p. 282)	
				aws:TagKeys (p. 282)	
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* (p. 282)		
CreateReportGroup	Grants permission to create a report group	Write	report-group* (p. 282)		
				aws:RequestTag/\${TagKey} (p. 282)	
				aws:TagKeys (p. 282)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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* (p. 282)		
DeleteBuildBatch	Grants permission to delete a build batch	Write	project* (p. 282)		
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* (p. 282)		
DeleteReport	Grants permission to delete a report	Write	report-group* (p. 282)		
DeleteReportGroup	Grants permission to delete a report group	Write	report-group* (p. 282)		
DeleteResourcePolicy	Grants permission to delete a resource policy for the associated project or report group	Permissions management	project (p. 282) report-group (p. 282)		
DeleteSourceCredentials	Grants permission to delete a set of GitHub, GitHub Enterprise, or Bitbucket source credentials	Write			
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* (p. 282)		
DescribeCodeCoverage	Grants permission to return an array of CodeCoverage objects	Read	report-group* (p. 282)		
DescribeTestCase	Grants permission to return an array of TestCase objects	Read	report-group* (p. 282)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetReportGroupTests	Grants permission to analyze and accumulate test report values for the test reports in the specified report group	Read	report-group* (p. 282)		
GetResourcePolicy	Grants permission to return a resource policy for the specified project or report group	Read	project (p. 282)		
			report-group (p. 282)		
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			
InvalidateProjectCache	Grants permission to reset the cache for a project	Write	project* (p. 282)		
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* (p. 282)		
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* (p. 282)		
ListConnectedOAuthProviders [permission only]	Grants permission to list third-party OAuth providers. Only used in the AWS CodeBuild console	List			
ListCuratedEnvironments	Grants permission to get information about Docker images that are managed by AWS CodeBuild	List			
ListProjects	Grants permission to get a list of build project names, with each build project name representing a single build project	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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* (p. 282)		
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			
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 (p. 282) report-group (p. 282)		
RetryBuild	Grants permission to retry a build	Write	project* (p. 282)		
RetryBuildBatch	Grants permission to retry a build batch	Write	project* (p. 282)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartBuild	Grants permission to start running a build	Write	project* (p. 282)		
StartBuildBatch	Grants permission to start running a build batch	Write	project* (p. 282)		
StopBuild	Grants permission to attempt to stop running a build	Write	project* (p. 282)		
StopBuildBatch	Grants permission to attempt to stop running a build batch	Write	project* (p. 282)		
UpdateProject	Grants permission to change the settings of an existing build project	Write	project* (p. 282)		
				aws:RequestTag/\${TagKey} (p. 282)	
				aws:TagKeys (p. 282)	
UpdateProjectVisibility	Grants permission to change the public visibility of a project and its builds	Write	project* (p. 282)		
				aws:RequestTag/\${TagKey} (p. 282)	
				aws:TagKeys (p. 282)	
UpdateReport [permission only]	Grants permission to update information about a report	Write	report-group* (p. 282)		
UpdateReportGroup	Grants permission to change the settings of an existing report group	Write	report-group* (p. 282)		
				aws:RequestTag/\${TagKey} (p. 282)	
				aws:TagKeys (p. 282)	
UpdateWebhook	Grants permission to update the webhook associated with an AWS CodeBuild build project	Write	project* (p. 282)		

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 \(p. 276\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 282)
report-group	arn:\${Partition}:codebuild:\${Region}: \${Account}:report-group/\${ReportGroupName}	aws:ResourceTag/\${TagKey} (p. 282)
report	arn:\${Partition}:codebuild:\${Region}: \${Account}:report/\${ReportGroupName}: \${ReportId}	

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 [Available global condition 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 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 \(p. 283\)](#)

- [Resource types defined by AWS CodeCommit \(p. 291\)](#)
- [Condition keys for AWS CodeCommit \(p. 292\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 291)		
BatchAssociateApprovalRuleTemplateWithRepositories	Grants permission to associate an approval rule template with multiple repositories in a single operation	Write	repository* (p. 291)		
BatchDescribeMergeInformation	Grants permission to get information about multiple merge conflicts when attempting to merge two commits using either the three-way merge or the squash merge option	Read	repository* (p. 291)		
BatchDisassociateApprovalRuleFromRepositories	Grants permission to remove the association between an approval rule template and multiple repositories in a single operation	Write	repository* (p. 291)		
BatchGetCommits	Grants permission to get return information about one or more commits in an AWS CodeCommit repository	Read	repository* (p. 291)		
BatchGetPullRequests [permission only]	Grants permission to return information about one or more pull requests in an AWS CodeCommit repository	Read	repository* (p. 291)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetRepository	Grants permission to get information about multiple repositories	Read	repository* (p. 291)		
CancelUploadArchive [permission only]	Grants permission to cancel the uploading of an archive to a pipeline in AWS CodePipeline	Read	repository* (p. 291)		
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		repository* (p. 291)		codecommit:References (p. 292)
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* (p. 291)		codecommit:References (p. 292)
CreatePullRequest	Grants permission to create a pull request in the specified repository		repository* (p. 291)		
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* (p. 291)		
CreateRepository	Grants permission to create an AWS CodeCommit repository	Write	repository* (p. 291)		
					aws:RequestTag/\${TagKey} (p. 292)
CreateUnreferencedMergeCommit	Grants permission to create a merge 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* (p. 291)		
					codecommit:References (p. 292)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteApprovalRuleTemplate	Grants permission to delete an approval rule template	Write			
DeleteBranch	Grants permission to delete a branch in an AWS CodeCommit repository with this API; does not control Git delete branch actions	Write	repository* (p. 291)		
					codecommit:References (p. 292)
DeleteCommentContent	Grants permission to delete the content of a comment made on a change, file, or commit in a repository	Write	repository* (p. 291)		
DeleteFile	Grants permission to delete a specified file from a specified branch	Write	repository* (p. 291)		
					codecommit:References (p. 292)
DeletePullRequestApprovalRule	Grants permission to delete an approval rule created for a pull request if the rule was not created by an approval rule template	Write	repository* (p. 291)		
DeleteRepository	Grants permission to delete an AWS CodeCommit repository	Write	repository* (p. 291)		
DescribeMergeConflict	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* (p. 291)		
DescribePullRequestInformation	Grants permission to return information about one or more pull request events	Read	repository* (p. 291)		
DisassociateApprovalRuleTemplateFromRepository	Grants permission to remove the association between an approval rule template and a repository	Write	repository* (p. 291)		
EvaluatePullRequestMergeability	Grants permission to evaluate whether a pull request is mergeable based on its current approval state and approval rule requirements	Read	repository* (p. 291)		
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* (p. 291)		
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* (p. 291)		
GetComment	Grants permission to get the content of a comment made on a change, file, or commit in a repository	Read	repository* (p. 291)		
GetCommentReactions	Grants permission to get reactions on a comment	Read	repository* (p. 291)		
GetCommentsForComparison	Grants permission to get information about comments made on the comparison between two commits	Read	repository* (p. 291)		
GetCommentsForPullRequest	Grants permission to get comments made on a pull request	Read	repository* (p. 291)		
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* (p. 291)		
GetCommitHistory [permission only]	Grants permission to get information about the history of commits in a repository	Read	repository* (p. 291)		
GetCommitsFromMergeInformation [permission only]	Grants permission to get information about the difference between commits in the context of a potential merge	Read	repository* (p. 291)		
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* (p. 291)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetFile	Grants permission to return the base-64 encoded contents of a specified file and its metadata	Read	repository* (p. 291)		
GetFolder	Grants permission to return the contents of a specified folder in a repository	Read	repository* (p. 291)		
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* (p. 291)		
GetMergeConflict			repository* (p. 291)	codecommit:References (p. 292)	
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* (p. 291)		
GetObjectIdentifier [permission only]	Grants permission to resolve blobs, trees, and commits to their identifier	Read	repository* (p. 291)		
GetPullRequest	Grants permission to get information about a pull request in a specified repository	Read	repository* (p. 291)		
GetPullRequestApprovals	Grants permission to retrieve the current approvals on an inputted pull request	Read	repository* (p. 291)		
GetPullRequestOverride	Grants permission to retrieve the current override state of a given pull request	Read	repository* (p. 291)		
GetReferences [permission only]	Grants permission to get details about references in an AWS CodeCommit repository; does not control Git reference actions	Read	repository* (p. 291)		
GetRepository	Grants permission to get information about an AWS CodeCommit repository	Read	repository* (p. 291)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRepositoryTriggers	Grants permission to get information about triggers configured for a repository	Read	repository* (p. 291)		
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* (p. 291)		
GetUploadArchiveInformation [permission only]	Grants permission to get status information about an archive upload to a pipeline in AWS CodePipeline	Read	repository* (p. 291)		
GitPull [permission only]	Grants permission to pull information from an AWS CodeCommit repository to a local repo	Read	repository* (p. 291)		
GitPush [permission only]	Grants permission to push information from a local repo to an AWS CodeCommit repository	Write	repository* (p. 291)		
					codecommit:References (p. 292)
ListApprovalRuleTemplates	Grants permission to list all approval rule templates in an AWS Region for the AWS account	List			
ListAssociatedApprovalRuleTemplateRepositories	Grants permission to list approval rule template repositories associated with a repository	List	repository* (p. 291)		
ListBranches	Grants permission to list branches for an AWS CodeCommit repository with this API; does not control Git branch actions	List	repository* (p. 291)		
ListPullRequests	Grants permission to list pull requests for a specified repository	List	repository* (p. 291)		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to list the resource attached to a CodeCommit resource ARN	List	repository (p. 291)		
MergeBranchesByFastForward	Grants permission to merge two commits into the specified destination branch using the fast-forward merge option	Write	repository* (p. 291)		
				codecommit:References (p. 292)	
MergeBranchesBySquash	Grants permission to merge two commits into the specified destination branch using the squash merge option	Write	repository* (p. 291)		
				codecommit:References (p. 292)	
MergeBranchesByThreeWay	Grants permission to merge two commits into the specified destination branch using the three-way merge option	Write	repository* (p. 291)		
				codecommit:References (p. 292)	
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* (p. 291)		
				codecommit:References (p. 292)	
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* (p. 291)		
				codecommit:References (p. 292)	
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* (p. 291)		
				codecommit:References (p. 292)	
OverridePullRequestApprovalRules	Grants permission to override all approval rules for a pull request, including approval rules created by a template	Write	repository* (p. 291)		
PostCommentForComparison	Grants permission to post a comment on the comparison between two commits	Write	repository* (p. 291)		
PostCommentForPullRequest	Grants permission to post a comment on a pull request	Write	repository* (p. 291)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PostCommentReply	Grants permission to post a comment in reply to a comment on a comparison between commits or a pull request	Write	repository* (p. 291)		
PutCommentReaction	Grants permission to post a reaction on a comment	Write	repository* (p. 291)		
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* (p. 291)		
			codecommit:References (p. 292)		
PutRepositoryTrigger	Grants permission to create, update, or delete triggers for a repository	Write	repository* (p. 291)		
TagResource	Grants permission to attach resource tags to a CodeCommit resource ARN	Tagging	repository (p. 291)		
			aws:ResourceTag / {\$TagKey} (p. 292)		
			aws:RequestTag / {\$TagKey} (p. 292)		
			aws:TagKeys (p. 292)		
TestRepositoryTrigger	Grants permission to test the functionality of repository triggers by sending information to the trigger target	Write	repository* (p. 291)		
UntagResource	Grants permission to disassociate resource tags from a CodeCommit resource ARN	Tagging	repository (p. 291)		
			aws:TagKeys (p. 292)		
UpdateApprovalRuleContent	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			
UpdateApprovalRuleDescription	Grants permission to update the Description of approval rule templates	Write			
UpdateApprovalRuleName	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* (p. 291)		

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* (p. 291)		
UpdatePullRequestReviewRuleContentForApproval	Grants permission to update 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* (p. 291)		
UpdatePullRequestApprovalState	Grants permission to update the approval state for pull requests	Write	repository* (p. 291)		
UpdatePullRequestDescription	Grants permission to update the description of a pull request	Write	repository* (p. 291)		
UpdatePullRequestStatus	Grants permission to update the status of a pull request	Write	repository* (p. 291)		
UpdatePullRequestTitle	Grants permission to update the title of a pull request	Write	repository* (p. 291)		
UpdateRepositoryDescription	Grants permission to change the description of an AWS CodeCommit repository	Write	repository* (p. 291)		
UpdateRepositoryName	Grants permission to change the name of an AWS CodeCommit repository	Write	repository* (p. 291)		
UploadArchive [permission only]	Grants permission to the service role for AWS CodePipeline to upload repository changes into a pipeline	Write	repository* (p. 291)		

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 \(p. 283\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
repository	<code>arn:\${Partition}:codecommit:\${Region}:\${Account}://\${RepositoryName}</code>	aws:ResourceTag/\${TagKey} (p. 292)

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 [Available global condition 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
codecommit:ReferenceActions	Filters access by Git reference to specified AWS CodeCommit actions	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 \(p. 292\)](#)
- [Resource types defined by AWS CodeDeploy \(p. 297\)](#)
- [Condition keys for AWS CodeDeploy \(p. 298\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 298)		
BatchGetApplicationInformation	Grants permission to get information about one or more application revisions	Read	application* (p. 297)		
BatchGetApplicationInformation	Grants permission to get information about multiple applications associated with the IAM user	Read	application* (p. 297)		
BatchGetDeploymentInformation	Grants permission to get information about one or more deployment groups	Read	deploymentgroup* (p. 298)		
BatchGetDeploymentInformation	Grants permission to get information about one or more instance that are part of a deployment group	Read	deploymentgroup* (p. 298)		
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			
BatchGetDeploymentInformation	Grants permission to get information about multiple deployments associated with the IAM user	Read	deploymentgroup* (p. 298)		
BatchGetOnPremisesInstances	Grants permission to get information about one or more on-premises instances	Read	instance* (p. 298)		
ContinueDeployment	Grants permission to start the process of rerouting traffic from instances in the original environment to instances in the replacement environment without waiting for a specified wait time to elapse	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateApplication	Grants permission to create an application associated with the IAM user	Write	application* (p. 297)		
			aws:RequestTag/ \${TagKey} (p. 298)		
			aws:TagKeys (p. 298)		
CreateCloudFormationDeployment [permission only]	Grants permission to create a CloudFormation deployment to cooperate orchestration for a CloudFormation stack update	Write			
CreateDeployment	Grants permission to create a deployment for an application associated with the IAM user	Write	deploymentgroup* (p. 298)		
CreateDeploymentConfig	Grants permission to create a custom deployment configuration associated with the IAM user	Write	deploymentconfig* (p. 298)		
CreateDeploymentGroup	Grants permission to create a deployment group for an application associated with the IAM user	Write	deploymentgroup* (p. 298)		
			aws:RequestTag/ \${TagKey} (p. 298)		
			aws:TagKeys (p. 298)		
DeleteApplication	Grants permission to delete an application associated with the IAM user	Write	application* (p. 297)		
DeleteDeploymentConfig	Grants permission to delete a custom deployment configuration associated with the IAM user	Write	deploymentconfig* (p. 298)		
DeleteDeploymentGroup	Grants permission to delete a deployment group for an application associated with the IAM user	Write	deploymentgroup* (p. 298)		
DeleteGitHubAccount	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* (p. 298)		
GetApplication	Grants permission to get information about a single application associated with the IAM user	List	application* (p. 297)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetApplicationRevision	Grants permission to get information about a single application revision for an application associated with the IAM user	List	application* (p. 297)		
GetDeployment	Grants permission to get information about a single deployment to a deployment group for an application associated with the IAM user	List	deploymentgroup* (p. 298)		
GetDeploymentConfig	Grants permission to get information about a single deployment configuration associated with the IAM user	List	deploymentconfig* (p. 298)		
GetDeploymentGroup	Grants permission to get information about a single deployment group for an application associated with the IAM user	List	deploymentgroup* (p. 298)		
GetDeploymentInstance	Grants permission to get information about a single instance in a deployment associated with the IAM user	List	deploymentgroup* (p. 298)		
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* (p. 298)		
ListApplicationRevisions	Grants permission to get information about all application revisions for an application associated with the IAM user	List	application* (p. 297)		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDeploymentGroups	Grants permission to get information about all deployment groups for an application associated with the IAM user	List	application* (p. 297)		
ListDeploymentInstances	Grants permission to get information about all instances in a deployment associated with the IAM user	List	deploymentgroup* (p. 298)		
ListDeploymentTargets	Grants permission to return a list of target IDs that are associated with 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* (p. 298)		
ListGitHubAccounts	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 (p. 297)		
			deploymentgroup (p. 298)		
PutLifecycleEventHook	Grants permission to notify execution status for associated deployment with the IAM user	Write			
RegisterApplication	Grants permission to register information about an application revision for an application associated with the IAM user	Write	application* (p. 297)		
RegisterOnPremisesInstance	Grants permission to register an on-premises instance	Write	instance* (p. 298)		
RemoveTagsFromInstances	Grants permission to remove tags from one or more on-premises instances	Tagging	instance* (p. 298)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SkipWaitTimeForAnySpecifiedWaitTime	Grants permission to override <code>anySpecifiedWaitTime</code> and starts terminating instances immediately after the traffic routing is complete. This action applies to blue-green deployments only	Write			
StopDeployment	Grants permission to stop a deployment	Write			
TagResource	Grants permission to associate the list of tags in the input Tags parameter with the resource identified by the ResourceArn input parameter	Tagging	application (p. 297)		
			deploymentgroup (p. 298)		
				aws:RequestTag/\${TagKey} (p. 298)	aws:TagKeys (p. 298)
UntagResource	Grants permission to disassociate a resource from a list of tags. The resource is identified by the ResourceArn input parameter. The tags are identified by the list of keys in the TagKeys input parameter	Tagging	application (p. 297)		
			deploymentgroup (p. 298)		
				aws:TagKeys (p. 298)	
UpdateApplication	Grants permission to update an application	Write	application* (p. 297)		
UpdateDeployment	Grants permission to change information about a single deployment group for an application associated with the IAM user	Write	deploymentgroup* (p. 298)		

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](#) (p. 292) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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}	

Resource types	ARN	Condition keys
deploymentconfig	arn:\${Partition}:codedeploy:\${Region}:\${Account}:deploymentconfig:\${DeploymentConfigurationName}	
deploymentgroup	arn:\${Partition}:codedeploy:\${Region}:\${Account}:deploymentgroup:\${ApplicationName}/\${DeploymentGroupName}	
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 [Available global condition 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 \(p. 299\)](#)
- [Resource types defined by AWS CodeDeploy secure host commands service \(p. 299\)](#)
- [Condition keys for AWS CodeDeploy secure host commands service \(p. 299\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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			
PutHostCommandAcknowledgment	Grants permission to mark host agent commands acknowledged	Write			
PutHostCommandCompletion	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 [Available keys for conditions](#).

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 \(p. 300\)](#)
- [Resource types defined by Amazon CodeGuru \(p. 300\)](#)
- [Condition keys for Amazon CodeGuru \(p. 301\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
<code>GetCodeGuruFreeCodeGuruSession</code> [permission only]	Gets 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 [Available keys for conditions](#).

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 \(p. 301\)](#)
- [Resource types defined by Amazon CodeGuru Profiler \(p. 303\)](#)
- [Condition keys for Amazon CodeGuru Profiler \(p. 304\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddNotificationTopics	Grants permission to add up to 2 ARNs of existing AWS SNS topics to publish notifications	Write	ProfilingGroup* (p. 303)		
BatchGetFrameMetrics	Grants permission to get the metric data for a Profiling Group	List	ProfilingGroup* (p. 303)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ConfigureAgent [permission only]	Grants permission for an agent to register with the orchestration service and retrieve profiling configuration information	Write	ProfilingGroup* (p. 303)		
CreateProfilingGroup	Grants permission to create a profiling group	Write		aws:TagKeys (p. 304) aws:RequestTag/ \${TagKey} (p. 304)	
DeleteProfilingGroup	Grants permission to delete a profiling group	Write	ProfilingGroup* (p. 303)		
DescribeProfilingGroup	Grants permission to describe a profiling group	Read	ProfilingGroup* (p. 303)		
GetFindingsReport	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	ProfilingGroup* (p. 303)		
GetPolicy	Grants permission to get the resource policy associated with the specified Profiling Group	Read	ProfilingGroup* (p. 303)		
GetProfile	Grants permission to get aggregated profiles for a specific profiling group	Read	ProfilingGroup* (p. 303)		
GetRecommendations	Grants permission to get recommendations	Read	ProfilingGroup* (p. 303)		
ListFindingsReports	Grants permission to list the available recommendations reports for a specific profiling group	List	ProfilingGroup* (p. 303)		
ListProfileTimes	Grants permission to list the start times of the available aggregated profiles for a specific profiling group	List	ProfilingGroup* (p. 303)		
ListProfilingGroups	Grants permission to list the profiling groups in the account	List			
ListTagsForResource	Grants permission to list tags for a Profiling Group	List	ProfilingGroup* (p. 303)		
PostAgentProfile [permission only]	Grants permission to submit a profile collected by an agent belonging to a specific profiling group for aggregation	Write	ProfilingGroup* (p. 303)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	ProfilingGroup* (p. 303)		
RemoveNotificationTopic	Grants permission to delete an already configured SNS topic arn from the notification configuration	Write	ProfilingGroup* (p. 303)		
RemovePermission	Grants permission to remove the permission of specified Action Group from the resource policy associated with the specified Profiling Group	Permissions management	ProfilingGroup* (p. 303)		
SubmitFeedback	Grants permission to submit user feedback for useful or non useful anomaly	Write	ProfilingGroup* (p. 303)		
TagResource	Grants permission to add or overwrite tags to a Profiling Group	Tagging	ProfilingGroup* (p. 303)		
				aws:TagKeys (p. 304)	
				aws:RequestTag/\${TagKey} (p. 304)	
UntagResource	Grants permission to remove tags from a Profiling Group	Tagging	ProfilingGroup* (p. 303)		
				aws:TagKeys (p. 304)	
				aws:RequestTag/\${TagKey} (p. 304)	
UpdateProfilingGroup	Grants permission to update a specific profiling group	Write	ProfilingGroup* (p. 303)		

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 \(p. 301\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
ProfilingGroup	arn:\${Partition}:codeguru-profiler:\${Region}:\${Account}:profilingGroup/\${ProfilingGroupName}	aws:ResourceTag/\${TagKey} (p. 304)

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters actions based on the presence of tag key-value pairs in the request	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters actions based on tag key-value pairs attached to the resource	String
<code>aws:TagKeys</code>	Filters actions based on 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 \(p. 304\)](#)
- [Resource types defined by Amazon CodeGuru Reviewer \(p. 307\)](#)
- [Condition keys for Amazon CodeGuru Reviewer \(p. 307\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateRepository	Grants permission to associates a repository with Amazon CodeGuru Reviewer	Write	association* (p. 307)		codecommit>ListRepositories codecommitTagResource eventsPutRule eventsPutTargets iamCreateServiceLinkedRole s3CreateBucket s3ListBucket s3PutBucketPolicy s3PutLifecycleConfiguration
			connection (p. 307)		
			repository (p. 307)		
					awsRequestTag/\${TagKey} (p. 307) awsTagKeys (p. 307)
CreateCodeReview	Grants permission to create a code review	Write	association* (p. 307)		s3GetObject
CreateConnection	Grants permission to perform token-based oauth handshake for 3rd party providers [permission only]	Read			
DescribeCodeReview	Grants permission to describe a code review	Read	association* (p. 307)		
DescribeRecommendationFeedback	Grants permission to describe a recommendation feedback on a code review	Read	association* (p. 307)		
DescribeRepositoryAssociation	Grants permission to describe a repository association	Read	association* (p. 307)		
DisassociateRepository	Grants permission to disassociate a repository with Amazon CodeGuru Reviewer	Write	association* (p. 307)		codecommitUntagResource eventsDeleteRule eventsRemoveTargets

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/ \${TagKey} (p. 307)	
GetMetricsData [permission only]	Grants permission to view pull request metrics in console	Read			
ListCodeReviews	Grants permission to list summary of code reviews	List			
ListRecommendations	Grants permission to list summary of recommendation feedback on a code review	List	association* (p. 307)		
ListRecommendations	Grants permission to list summary of recommendations on a code review	List	association* (p. 307)		
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* (p. 307)		
ListThirdPartyRepositories	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* (p. 307)		
TagResource	Grants permission to attach resource tags to an associated repository ARN	Tagging	association* (p. 307)		
UnTagResource	Grants permission to disassociate resource tags from an associated repository ARN	Tagging	association* (p. 307)		

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 \(p. 304\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
association	<code>arn:\${Partition}:codeguru-reviewer:\${Region}:\${Account}:association:\${ResourceId}</code>	
codereview	<code>arn:\${Partition}:codeguru-reviewer:\${Region}:\${Account}:association:\${ResourceId}:codereview:\${CodeReviewId}</code>	
repository	<code>arn:\${Partition}:codecommit:\${Region}:\${Account}:\${RepositoryName}</code>	aws:ResourceTag/\${TagKey} (p. 307)
connection	<code>arn:\${Partition}:codestar-connections:\${Region}:\${Account}:connection/\${ConnectionId}</code>	

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters access based on the presence of tag key-value pairs in the request	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters actions based on tag key-value pairs attached to the resource	String
<code>aws:TagKeys</code>	Filters access based on the presence of tag keys 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 \(p. 308\)](#)
- [Resource types defined by AWS CodePipeline \(p. 312\)](#)
- [Condition keys for AWS CodePipeline \(p. 312\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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			
CreateCustomAction	Grants permission to create a <code>CustomType</code> action that you can use in the pipelines associated with your AWS account	Write	actiontype* (p. 312)		
			aws:RequestTag/\${TagKey} (p. 312)		aws:TagKeys (p. 312)
CreatePipeline	Grants permission to create a uniquely named pipeline	Write	pipeline* (p. 312)		
			aws:RequestTag/\${TagKey} (p. 312)		aws:TagKeys (p. 312)
DeleteCustomAction	Grants permission to delete a <code>CustomType</code> action	Write	actiontype* (p. 312)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeletePipeline	Grants permission to delete a specified pipeline	Write	pipeline* (p. 312)		
DeleteWebhook	Grants permission to delete a specified webhook	Write	webhook* (p. 312)		
DeregisterWebhookFromThirdParty	Grants permission to remove the registration of a webhook with the third party specified in its configuration	Write	webhook* (p. 312)		
DisableStageTransition	Grants permission to prevent revisions from transitioning to the next stage in a pipeline	Write	stage* (p. 312)		
EnableStageTransition	Grants permission to allow revisions to transition to the next stage in a pipeline	Write	stage* (p. 312)		
GetActionType	Grants permission to view information about an action type	Read			
GetJobDetails	Grants permission to view information about a job (custom actions only)	Read			
GetPipeline	Grants permission to retrieve information about a pipeline structure	Read	pipeline* (p. 312)		
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* (p. 312)		
GetPipelineState	Grants permission to view information about the current state of the stages and actions of a pipeline	Read	pipeline* (p. 312)		
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* (p. 312)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListActionTypes	Grants permission to list a summary of all the action types available for pipelines in your account	Read			
ListPipelineExecutions	Grants permission to list a summary of the most recent executions for a pipeline	List	pipeline* (p. 312)		
ListPipelines	Grants permission to list a summary of all the pipelines associated with your AWS account	List			
ListTagsForResource	Grants permission to list tags for a CodePipeline resource	Read	actiontype (p. 312)		
			pipeline (p. 312)		
			webhook (p. 312)		
ListWebhooks	Grants permission to list all of the webhooks associated with your AWS account	List	webhook* (p. 312)		
PollForJobs	Grants permission to view information about any jobs for CodePipeline to act on	Write	actiontype* (p. 312)		
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* (p. 312)		
PutApprovalResult	Grants permission to provide a response (Approved or Rejected) to a manual approval request in CodePipeline	Write	action* (p. 312)		
PutJobFailureResult	Grants permission to represent the failure of a job as returned to the pipeline by a job worker (custom actions only)	Write			
PutJobSuccessResult	Grants permission to represent the success of a job as returned to the pipeline by a job worker (custom actions only)	Write			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutThirdPartyJob	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* (p. 312)		
			webhook* (p. 312)		
			aws:RequestTag/\${TagKey} (p. 312) aws:TagKeys (p. 312)		
RegisterWebhook	Grants permission to register a webhook with the third party specified in its configuration	Write	webhook* (p. 312)		
RetryStageExecution	Grants permission to resume the pipeline execution by retrying the last failed actions in a stage	Write	stage* (p. 312)		
StartPipelineExecution	Grants permission to run the most recent revision through the pipeline	Write	pipeline* (p. 312)		
StopPipelineExecution	Grants permission to stop an in-progress pipeline execution	Write	pipeline* (p. 312)		
TagResource	Grants permission to tag a CodePipeline resource	Tagging	actiontype (p. 312)		
			pipeline (p. 312)		
			webhook (p. 312)		
			aws:RequestTag/\${TagKey} (p. 312) aws:TagKeys (p. 312)		
UntagResource	Grants permission to remove a tag from a CodePipeline resource	Tagging	actiontype (p. 312)		
			pipeline (p. 312)		
			webhook (p. 312)		
				aws:TagKeys (p. 312)	
UpdateActionType	Grants permission to update an action type	Write	actiontype* (p. 312)		
UpdatePipeline	Grants permission to update a pipeline with changes to the structure of the pipeline	Write	pipeline* (p. 312)		

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 \(p. 308\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
action	<code>arn:\${Partition}:codepipeline:\${Region}: \${Account}:\${PipelineName}/\${StageName}/ \${ActionName}</code>	aws:ResourceTag/\${TagKey} (p. 312)
actiontype	<code>arn:\${Partition}:codepipeline:\${Region}: \${Account}:actiontype:\${Owner}/\${Category}/ \${Provider}/\${Version}</code>	aws:ResourceTag/\${TagKey} (p. 312)
pipeline	<code>arn:\${Partition}:codepipeline:\${Region}: \${Account}:\${PipelineName}</code>	aws:ResourceTag/\${TagKey} (p. 312)
stage	<code>arn:\${Partition}:codepipeline:\${Region}: \${Account}:\${PipelineName}/\${StageName}</code>	aws:ResourceTag/\${TagKey} (p. 312)
webhook	<code>arn:\${Partition}:codepipeline:\${Region}: \${Account}:webhook:\${WebhookName}</code>	aws:ResourceTag/\${TagKey} (p. 312)

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 [Available global condition 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 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 \(p. 313\)](#)
- [Resource types defined by AWS CodeStar \(p. 315\)](#)
- [Condition keys for AWS CodeStar \(p. 315\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateTeamMember	Adds a user to the team for an AWS CodeStar project.	Permissions management	project* (p. 315)		
CreateProject	Creates a project with minimal structure, customer policies, and no resources.	Permissions management		aws:RequestTag/\${TagKey} (p. 315) aws:TagKeys (p. 316)	
CreateUserProfile	Creates a profile for a user that includes user preferences, display name, and email.	Write	user* (p. 315)		
DeleteExtendedAccess [permission only]	Grants access to extended delete access	Write	project* (p. 315)		
DeleteProject	Deletes 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* (p. 315)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteUserProfile	Deletes a user profile in AWS CodeStar, 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.	Write	user* (p. 315)		
DescribeProject	Describes a project and its resources.	Read	project* (p. 315)		
DescribeUserProfile	Describes a user in AWS CodeStar and the user attributes across all projects.	Read			
DisassociateTeam	Removes 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* (p. 315)		
GetExtendedAccessAPIs [permission only]	Grants access to extended read APIs.	Read	project* (p. 315)		
ListProjects	Lists all projects in CodeStar associated with your AWS account.	List			
ListResources	Lists all resources associated with a project in CodeStar.	List	project* (p. 315)		
ListTagsForProject	Lists the tags associated with a project in CodeStar.	List	project* (p. 315)		
ListTeamMembers	Lists all team members associated with a project.	List	project* (p. 315)		
ListUserProfiles	Lists user profiles in AWS CodeStar.	List			
PutExtendedAccessAPIs [permission only]	Grants access to extended write APIs.	Write	project* (p. 315)		
TagProject	Adds tags to a project in CodeStar.	Tagging	project* (p. 315)	aws:RequestTag/ \${TagKey} (p. 315) aws:TagKeys (p. 316)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagProject	Removes tags from a project in CodeStar.	Tagging	project* (p. 315)		
			aws:TagKeys (p. 316)		
UpdateProject	Updates a project in CodeStar.	Write	project* (p. 315)		
UpdateTeamMember	Updates team member attributes within a CodeStar project.	Permissions management	project* (p. 315)		
UpdateUserProfile	Updates a profile for a user that includes user preferences, display name, and email.	Write	user* (p. 315)		
VerifyServiceRole	Verifies 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 \(p. 313\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 315)
user	arn:\${Partition}:iam::\${Account}:user/ \${aws:username}	iam:ResourceTag/ \${TagKey} (p. 316)

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 [Available global condition 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

Condition keys	Description	Type
aws:TagKeys	Filters create requests based on the presence of mandatory tags in the request.	String
iam:ResourceTag/\${TagKey}		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 \(p. 316\)](#)
- [Resource types defined by AWS CodeStar Connections \(p. 319\)](#)
- [Condition keys for AWS CodeStar Connections \(p. 319\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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} (p. 319) aws:TagKeys (p. 319)	

Service Authorization Reference
Service Authorization Reference
AWS CodeStar Connections

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codestar-connections:ProviderType (p. 320)	
CreateHost	Grants permission to create a host resource	Write		aws:RequestTag/\${TagKey} (p. 319) aws:TagKeys (p. 319) codestar-connections:ProviderType (p. 320)	
DeleteConnection	Grants permission to delete a Connection resource	Write	Connection* (p. 319)		
DeleteHost	Grants permission to delete a host resource	Write	Host* (p. 319)		
GetConnection	Grants permission to get details about a Connection resource	Read	Connection* (p. 319)		
GetHost	Grants permission to get details about a host resource	Read	Host* (p. 319)		
GetIndividualAccess [permission only]	Grants permission to associate a third party, such as a Bitbucket App installation, with a Connection	Read		codestar-connections:ConnectionsStartOAuthFlow (p. 320)	
GetInstallationUrl [permission only]	Grants permission to associate a third party, such as a Bitbucket App installation, with a Connection	Read		codestar-connections:ProviderType (p. 320)	
ListConnections	Grants permission to list Connection resources	List		codestar-connections:ProviderTypeFilter (p. 320)	
ListHosts	Grants permission to list host resources	List		codestar-connections:ProviderTypeFilter (p. 320)	
ListInstallationTargets [permission only]	Grants permission to associate a third party, such as a Bitbucket App installation, with a Connection	List		codestar-connections:GetIndividualAccess (p. 320)	codestar-connections:StartOAuthFlow (p. 320)
ListTagsForResource	Gets the set of key-value pairs that are used to manage the resource	List	Connection* (p. 319)		
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* (p. 319)		
					codestar-connections:PassedToService (p. 320)

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 (p. 320)		
StartAppRegistration [permission only]	Grants permission to associate a third party server, such as a GitHub Enterprise Server instance, with a Host	Read		codestar-connections:HostArn (p. 320)		
StartOAuthHandshake [permission only]	Grants permission to associate a third party, such as a Bitbucket App installation, with a Connection	Read		codestar-connections:ProviderType (p. 320)		
TagResource	Adds to or modifies the tags of the given resource	Tagging	Connection* (p. 319)			
UntagResource	Removes tags from an AWS resource		aws:TagKeys (p. 319)			
			aws:RequestTag/ \${TagKey} (p. 319)			
			aws:TagKeys (p. 319)			
UpdateConnection	Grants permission to update a Connection resource with an installation of the CodeStar Connections App	Write	Connection* (p. 319)	codestar-connections:GetIndividualConnection		
			codestar-connections:GetInstallationId	codestar-connections>ListInstallations		
UpdateHost	Grants permission to update a host resource	Write	Host* (p. 319)	codestar-connections:InstallationId (p. 320)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UseConnection [permission only]	Grants permission to use a Connection resource to call provider actions	Read	Connection* (p. 319)	codestar-connections:FullRepositoryId (p. 320) codestar-connections:ProviderAction (p. 320) codestar-connections:ProviderPermissionsRequest (p. 320)	

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 \(p. 316\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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}	
Host	arn:\${Partition}:codestar-connections:\${Region}:\${Account}:host/\${HostId}	

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 [Available global condition 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
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

Condition keys	Description	Type
codestar-connections:FullRepositoryArn	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	String
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
codestar-connections:PassedToRequest	Filters access by the service to which the principal is allowed to pass a Connection	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:ProviderType	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:ProviderTypeFilter	Filters access by the type of third-party provider passed in the request	String
codestar-connections:RepositoryName	Filters access by the type of third-party provider used to filter results	String
codestar-connections:RepositoryRequest	Filters access by the repository name that is passed in the request. Applies only to UseConnection requests for creating new repositories	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 \(p. 321\)](#)
- [Resource types defined by AWS CodeStar Notifications \(p. 323\)](#)
- [Condition keys for AWS CodeStar Notifications \(p. 323\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 323) aws:RequestTag/\${TagKey} (p. 323) aws:TagKeys (p. 324) codestar-notifications:NotificationsForResource		
DeleteNotificationRule	Grants permission to delete a notification rule for a resource	Write	notificationrule* (p. 323) aws:ResourceTag/\${TagKey} (p. 323) aws:RequestTag/\${TagKey} (p. 323) aws:TagKeys (p. 324) codestar-notifications:NotificationsForResource		
DeleteTarget	Grants permission to delete a target for a notification rule	Write		aws:RequestTag/\${TagKey} (p. 323) aws:TagKeys (p. 324)	
DescribeNotificationRule	Grants permission to get information about a notification rule	Read	notificationrule* (p. 323) aws:ResourceTag/\${TagKey} (p. 323) aws:RequestTag/\${TagKey} (p. 323) aws:TagKeys (p. 324)		

Service Authorization Reference
Service Authorization Reference
AWS CodeStar Notifications

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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* (p. 323) aws:RequestTag/\${TagKey} (p. 323) aws:TagKeys (p. 324)		
ListTargets	Grants permission to list the notification rule targets for an AWS account	List		aws:RequestTag/\${TagKey} (p. 323) aws:TagKeys (p. 324)	
Subscribe	Grants permission to create an association between a notification rule and an Amazon SNS topic	Write	notificationrule* (p. 323) aws:ResourceTag/\${TagKey} (p. 323) aws:RequestTag/\${TagKey} (p. 323) aws:TagKeys (p. 324) codestar-notifications:NotificationsForResource		
TagResource	Grants permission to attach resource tags to a notification rule resource ARN	Tagging	notificationrule* (p. 323) aws:ResourceTag/\${TagKey} (p. 323) aws:RequestTag/\${TagKey} (p. 323) aws:TagKeys (p. 324)		
Unsubscribe	Grants permission to remove an association between a notification rule and an Amazon SNS topic	Write	notificationrule* (p. 323) aws:ResourceTag/\${TagKey} (p. 323) aws:RequestTag/\${TagKey} (p. 323) aws:TagKeys (p. 324) codestar-notifications:NotificationsForResource		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagResource	Grants permission to disassociate resource tags from a notification rule resource ARN	Tagging	notificationrule* (p. 323)		
				aws:RequestTag/ \${TagKey} (p. 323)	aws:TagKeys (p. 324)
UpdateNotificationRule	Grants permission to change a notification rule for a resource	Write	notificationrule* (p. 323)		
				aws:ResourceTag/ \${TagKey} (p. 323)	
				aws:RequestTag/ \${TagKey} (p. 323)	
				aws:TagKeys (p. 324)	
				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 \(p. 321\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 323)

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 [Available global condition keys](#).

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

Condition keys	Description	Type
aws:TagKeys	Filters actions based on the presence of tag keys in the request	ArrayOfString
codestar-notifications:NotificationArn	Filters access based on the ARN of the resource for which notifications are configured	ARN

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 \(p. 324\)](#)
- [Resource types defined by Amazon Cognito Identity \(p. 327\)](#)
- [Condition keys for Amazon Cognito Identity \(p. 327\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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} (p. 327) aws:TagKeys (p. 327)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteIdentities	Grants permission to delete identities from an identity pool. You can specify a list of 1-60 identities that you want to delete	Write			
DeleteIdentityPool	Grants permission to delete a user pool. Once a pool is deleted, users will not be able to authenticate with the pool	Write	identitypool* (p. 327)		
DescribeIdentity	Grants permission to return metadata related to the given identity, including when the identity was created and any associated linked logins	Read			
DescribeIdentityPool	Grants permission to get details about a particular identity pool, including the pool name, ID, description, creation date, and current number of users	Read	identitypool* (p. 327)		
GetCredentialsForIdentity	Grants permission to return credentials for the provided identity ID	Read			
GetId	Grants permission to generate (or retrieve) a Cognito ID. Supplying multiple logins will create an implicit linked account	Write			
GetIdentityPoolRoles	Grants permission to get the roles for an identity pool	Read	identitypool* (p. 327)		
GetOpenIdToken	Grants permission to get an OpenID token, using a known Cognito ID	Read			
GetOpenIdTokenForDeveloperIdentity	Grants permission to register (or retrieve) a Cognito IdentityId and an OpenID Connect token for a user authenticated by your backend authentication process	Read	identitypool* (p. 327)		
GetPrincipalTagAttributes	Grants permission to get the principal tags for an identity pool and provider	Read	identitypool* (p. 327)		
ListIdentities	Grants permission to list the identities in an identity pool	List	identitypool* (p. 327)		
ListIdentityPools	Grants permission to list all of the Cognito identity pools registered for your account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to list the tags that are assigned to an Amazon Cognito identity pool	Read	identitypool (p. 327)		
LookupDeveloperIdentity	Grants permission to retrieve the <code>IdentityId</code> associated with a <code>DeveloperUserIdentity</code> or the list of <code>DeveloperUserIdentities</code> associated with an <code>IdentityId</code> for an existing identity	Read	identitypool* (p. 327)		
MergeDeveloperIdentities	Grants permission to merge two users having different <code>IdentityIds</code> , existing in the same identity pool, and identified by the same developer provider	Write	identitypool* (p. 327)		
SetIdentityPoolRoles	Grants permission to set the roles for an identity pool. These roles are used when making calls to <code>GetCredentialsForIdentity</code> action	Write			
SetPrincipalTagAttribute	Grants permission to set the principal tags for an identity pool and provider. These tags are used when making calls to <code>GetOpenIdToken</code> action	Write			
TagResource	Grants permission to assign a set of tags to an Amazon Cognito identity pool	Tagging	identitypool (p. 327)		
			aws:RequestTag/\${TagKey} (p. 327)		aws:TagKeys (p. 327)
UnlinkDeveloperIdentity	Grants permission to unlink a <code>DeveloperUserIdentity</code> from an existing identity	Write	identitypool* (p. 327)		
UnlinkIdentity	Grants permission to unlink a federated identity from an existing account	Write			
UntagResource	Grants permission to remove the specified tags from an Amazon Cognito identity pool	Tagging	identitypool (p. 327)		
				aws:TagKeys (p. 327)	
UpdateIdentityPool	Grants permission to update an identity pool	Write	identitypool* (p. 327)		

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 \(p. 324\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
identitypool	<code>arn:\${Partition}:cognito-identity:\${Region}:\${Account}:identitypool/\${IdentityPoolId}</code>	aws:ResourceTag/\${TagKey} (p. 327)

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 [Available global condition keys](#).

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

Actions, resources, and condition keys for Amazon 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 \(p. 328\)](#)
- [Resource types defined by Amazon Cognito Sync \(p. 329\)](#)
- [Condition keys for Amazon Cognito Sync \(p. 330\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 330)		
DeleteDataset	Grants permission to delete a specific dataset	Write	dataset* (p. 330)		
DescribeDataset	Grants permission to get metadata about a dataset by identity and dataset name	Read	dataset* (p. 330)		
DescribeIdentityPoolUsage	Grants permission to get usage details (for example, data storage) about a particular identity pool	Read	identitypool* (p. 330)		
DescribeIdentityUser	Grants permission to get usage information for an identity, including number of datasets and data usage	Read	identity* (p. 330)		
GetBulkPublishDetails	Grants permission to get the status of the last BulkPublish operation for an identity pool	Read	identitypool* (p. 330)		
GetCognitoEvents	Grants permission to get the events and the corresponding Lambda functions associated with an identity pool	Read	identitypool* (p. 330)		
GetIdentityPoolConfiguration	Grants permission to get the configuration settings of an identity pool	Read	identitypool* (p. 330)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDatasets	Grants permission to list datasets for an identity	List	dataset* (p. 330)		
ListIdentityPoolUsers	Grants permission to get a list of identity pools registered with Cognito	Read	identitypool* (p. 330)		
ListRecords	Grants permission to get paginated records, optionally changed after a particular sync count for a dataset and identity	Read	dataset* (p. 330)		
QueryRecords [permission only]	Grants permission to query records	Read			
RegisterDevice	Grants permission to register a device to receive push sync notifications	Write	identity* (p. 330)		
SetCognitoEvents	Grants permission to set the AWS Lambda function for a given event type for an identity pool	Write	identitypool* (p. 330)		
SetDatasetConfigurations [permission only]	Grants permission to configure datasets	Write	dataset* (p. 330)		
SetIdentityPoolConfiguration	Grants permission to set the configuration for push sync	Write	identitypool* (p. 330)		
SubscribeToDataset	Grants permission to subscribe to receive notifications when a dataset is modified by another device	Write	dataset* (p. 330)		
UnsubscribeFromDataset	Grants permission to unsubscribe from receiving notifications when a dataset is modified by another device	Write	dataset* (p. 330)		
UpdateRecords	Grants permission to post updates to records and add and delete records for a dataset and user	Write	dataset* (p. 330)		

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 \(p. 328\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you

can include in a policy. These keys are displayed in the last column of the 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 [Available keys for conditions](#).

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 \(p. 330\)](#)
- [Resource types defined by Amazon Cognito User Pools \(p. 337\)](#)
- [Condition keys for Amazon Cognito User Pools \(p. 337\)](#)

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

policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddCustomAttributes	Adds additional user attributes to the user pool schema	Write	userpool* (p. 337)		
AdminAddUserToGroup	Adds the specified user to the specified group	Write	userpool* (p. 337)		
AdminConfirmSignUp	Confirms user registration as an admin without using a confirmation code. Works on any user	Write	userpool* (p. 337)		
AdminCreateUser	Creates a new user in the specified user pool and sends a welcome message via email or phone (SMS)	Write	userpool* (p. 337)		
AdminDeleteUser	Deletes a user as an administrator. Works on any user	Write	userpool* (p. 337)		
AdminDeleteUserAttributes	Deletes the user attributes in a user pool as an administrator. Works on any user	Write	userpool* (p. 337)		
AdminDisableProviderLink	Disables the user from signing in with the specified external (SAML or social) identity provider	Write	userpool* (p. 337)		
AdminDisableUser	Disables the specified user as an administrator. Works on any user	Write	userpool* (p. 337)		
AdminEnableUser	Enables the specified user as an administrator. Works on any user	Write	userpool* (p. 337)		
AdminForgetDevice	Forgets the device, as an administrator	Write	userpool* (p. 337)		
AdminGetDevice	Gets the device, as an administrator	Read	userpool* (p. 337)		
Admin GetUser	Gets the specified user by user name in a user pool as an administrator. Works on any user	Read	userpool* (p. 337)		
AdminInitiateAuth	Authenticates a user in a user pool as an administrator. Works on any user	Write	userpool* (p. 337)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AdminLinkProviderInUserPool	Links an existing user account (<code>DestinUser</code>) to an identity from an external identity provider (<code>SourceUser</code>) based on a specified attribute name and value from the external identity provider	Write	userpool* (p. 337)		
AdminListDevices	Lists devices, as an administrator	List	userpool* (p. 337)		
AdminListGroups	Lists the groups that the user belongs to	List	userpool* (p. 337)		
AdminListUserAuthEvents	Lists the authentication events for the user	Read	userpool* (p. 337)		
AdminRemoveUserFromGroup	Removes the specified user from the specified group	Write	userpool* (p. 337)		
AdminResetUserPassword	Resets the specified user's password in a user pool as an administrator. Works on any user	Write	userpool* (p. 337)		
AdminRespondToChallenge	Responds to an authentication challenge as an administrator	Write	userpool* (p. 337)		
AdminSetUserMFAPreference	Sets MFA preference for the user in the user pool	Write	userpool* (p. 337)		
AdminSetUserPassword	Sets the specified user's password in a user pool as an administrator. Works on any user	Write	userpool* (p. 337)		
AdminSetUserSettings	Sets all the user settings for a specified user name. Works on any user	Write	userpool* (p. 337)		
AdminUpdateAuthEventFeedback	Updates the feedback for the user authentication event	Write	userpool* (p. 337)		
AdminUpdateDeviceStatus	Updates the device status as an administrator	Write	userpool* (p. 337)		
AdminUpdateUserAttributes	Updates the specified user's attributes including developer attributes, as an administrator	Write	userpool* (p. 337)		
AdminUserGlobalSignOut	Signs out users from all devices, as an administrator	Write	userpool* (p. 337)		
AssociateSoftwareToken	Returns a unique generated shared secret key code for the user account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ChangePassword	Changes the password for a specified user in a user pool	Write			
ConfirmDevice	Confirms tracking of the device. This API call is the call that begins device tracking	Write			
ConfirmForgotPassword	Allows a user to enter a confirmation code to reset a forgotten password	Write			
ConfirmSignUp	Confirms registration of a user and handles the existing alias from a previous user	Write			
CreateGroup	Creates a new group in the specified user pool	Write	userpool* (p. 337)		
CreateIdentityProvider	Creates an identity provider for a user pool	Write	userpool* (p. 337)		
CreateResourceServer	Creates a new OAuth2.0 resource server and defines custom scopes in it	Write	userpool* (p. 337)		
CreateUserImportJob	Creates the user import job	Write	userpool* (p. 337)		
CreateUserPool	Creates a new Amazon Cognito user pool and sets the password policy for the pool	Write		aws:RequestTag/\${TagKey} (p. 338) aws:TagKeys (p. 338) aws:ResourceTag/\${TagKey} (p. 338)	
CreateUserPoolClient	Creates the user pool client	Write	userpool* (p. 337)		
CreateUserPoolDomain	Creates a new domain for a user pool	Write	userpool* (p. 337)		
DeleteGroup	Deletes a group. Currently only groups with no members can be deleted	Write	userpool* (p. 337)		
DeleteIdentityProvider	Deletes an identity provider for a user pool	Write	userpool* (p. 337)		
DeleteResourceServer	Deletes a resource server	Write	userpool* (p. 337)		
DeleteUser	Allows a user to delete one's self	Write			
DeleteUserAttributes	Deletes the attributes for a user	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteUserPool	Deletes the specified Amazon Cognito user pool	Write	userpool* (p. 337)		
DeleteUserPoolClient	Allows the developer to delete the user pool client	Write	userpool* (p. 337)		
DeleteUserPoolDomain	Deletes a domain for a user pool	Write	userpool* (p. 337)		
DescribeIdentityProvider	Gets information about a specific identity provider	Read	userpool* (p. 337)		
DescribeResourceServer	Describes a resource server	Read	userpool* (p. 337)		
DescribeRiskConfiguration	Describes the risk configuration setting for the userpool / userpool client	Read	userpool* (p. 337)		
DescribeUserImportJob	Describes the user import job	Read	userpool* (p. 337)		
DescribeUserPool	Returns the configuration information and metadata of the specified user pool	Read	userpool* (p. 337)		
DescribeUserPoolClient	Client method for returning the configuration information and metadata of the specified user pool client	Read	userpool* (p. 337)		
DescribeUserPoolDomain	Gets information about a domain	Read			
ForgetDevice	Forgets the specified device	Write			
ForgotPassword	Calling this API causes a message to be sent to the end user with a confirmation code that is required to change the user's password	Write			
GetCSVHeader	Gets the header information for the .csv file to be used as input for the user import job	Read	userpool* (p. 337)		
GetDevice	Gets the device	Read			
GetGroup	Gets a group	Read	userpool* (p. 337)		
GetIdentityProviderIdentifier	Gets the specified identity provider identifier	Read	userpool* (p. 337)		
GetSigningCertificate	Returns the signing certificate	Read	userpool* (p. 337)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetUICustomization	Gets the UI Customization information for a particular app client's app UI, if there is something set	Read	userpool* (p. 337)		
 GetUser	Gets the user attributes and metadata for a user	Read			
 GetUserAttributeVerificationCode	Gets the user attribute VerificationCode for the specified attribute name	Read			
 GetUserPoolMfaConfig	Gets the MFA configuration for the user pool	Read	userpool* (p. 337)		
 GlobalSignOut	Signs out users from all devices	Write			
 InitiateAuth	Initiates the authentication flow	Write			
 ListDevices	Lists the devices	List			
 ListGroups	Lists the groups associated with a user pool	List	userpool* (p. 337)		
 ListIdentityProviders	Lists information about all identity providers for a user pool	List	userpool* (p. 337)		
 ListResourceServers	Lists the resource servers for a user pool	List	userpool* (p. 337)		
 ListTagsForResource	Lists the tags that are assigned to an Amazon Cognito user pool	List	userpool (p. 337)		
 ListUserImportJobs	Lists the user import jobs	List	userpool* (p. 337)		
 ListUserPoolClients	Lists the clients that have been created for the specified user pool	List	userpool* (p. 337)		
 ListUserPools	Lists the user pools associated with an AWS account	List			
 ListUsers	Lists the users in the Amazon Cognito user pool	List	userpool* (p. 337)		
 ListUsersInGroup	Lists the users in the specified group	List	userpool* (p. 337)		
 ResendConfirmationCode	Resends the confirmation (for confirmation of registration) to a specific user in the user pool	Write			
 RespondToAuthChallenge	Responds to the authentication challenge	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RevokeToken	Revokes all of the access tokens generated by the specified refresh token	Write			
SetRiskConfiguration	sets the risk configuration setting for the userpool / userpool client	Write	userpool* (p. 337)		
SetUICustomization	Sets the UI customization information for a user pool's built-in app UI	Write	userpool* (p. 337)		
SetUserMFAPreference	Sets MFA preference for the user in the userpool	Write			
SetUserPoolMfaConfig	Sets the MFA configuration for the userpool	Write	userpool* (p. 337)		
SetUserSettings	Sets the user settings like multi-factor authentication (MFA)	Write			
SignUp	Registers the user in the specified user pool and creates a user name, password, and user attributes	Write			
StartUserImportJob	Starts the user import	Write	userpool* (p. 337)		
StopUserImportJob	Stops the user import job	Write	userpool* (p. 337)		
TagResource	Assigns a set of tags to an Amazon Cognito user pool	Tagging	userpool (p. 337)		
			aws:RequestTag/ \${TagKey} (p. 338)		aws:TagKeys (p. 338)
UntagResource	Removes the specified tags from an Amazon Cognito user pool	Tagging	userpool (p. 337)		
			aws:TagKeys (p. 338)		
UpdateAuthEventFeedback	Updates the feedback for the user authentication event	Write	userpool* (p. 337)		
UpdateDeviceStatus	Updates the device status	Write			
UpdateGroup	Updates the specified group with the specified attributes	Write	userpool* (p. 337)		
UpdateIdentityProviderInformation	Updates identity provider information for a user pool	Write	userpool* (p. 337)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateResourceServer	Updates the name and scopes of your resource server	Write	userpool* (p. 337)		
UpdateUserAttribute	Allows a user to update a specific attribute (one at a time)	Write			
UpdateUserPool	Updates the specified user pool with the specified attributes	Write	userpool* (p. 337)		
				aws:RequestTag/\${TagKey} (p. 338)	
				aws:TagKeys (p. 338)	
UpdateUserPoolClient	Allows the developer to update the specified user pool client and password policy	Write	userpool* (p. 337)		
UpdateUserPoolDomain	Updates the Secure Sockets Layer (SSL) certificate for the custom domain for your user pool	Write	userpool* (p. 337)		
VerifySoftwareToken	Registers a user's entered TOTP code and mark the user's software token MFA status as verified if successful	Write			
VerifyUserAttribute	Verifies 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 \(p. 330\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
userpool	<code>arn:\${Partition}:cognito-idp:\${Region}:\${Account}:userpool/\${UserPoolId}</code>	aws:ResourceTag/\${TagKey} (p. 338)

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 [Available global condition keys](#).

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

Actions, resources, and condition keys for Amazon 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 \(p. 338\)](#)
- [Resource types defined by Amazon Comprehend \(p. 350\)](#)
- [Condition keys for Amazon Comprehend \(p. 351\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 languages present in the list of text documents	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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* (p. 351)		
ContainsPiiEntities	Grants permission to classify the personally identifiable information within given documents in real-time	Read			
CreateDocumentClassifier	Grants permission to create a new document classifier that you can use to categorize documents	Write	document-classifier* (p. 351)		
				aws:RequestTag/\${TagKey} (p. 352) aws:TagKeys (p. 352) comprehend:VolumeKmsKey (p. 352) comprehend:ModelKmsKey (p. 352) comprehend:OutputKmsKey (p. 352) comprehend:VpcSecurityGroupIds (p. 352) comprehend:VpcSubnets (p. 352)	
CreateEndpoint	Grants permission to create a model-specific endpoint for synchronous inference for a previously trained custom model	Write	document-classifier* (p. 351)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			document-classifier-endpoint* (p. 351)		
			entity-recognizer* (p. 351)		
			entity-recognizer-endpoint* (p. 351)		
	Grants permission to create an entity recognizer using submitted files	Write	entity-recognizer* (p. 351)		
			aws:RequestTag/\${TagKey} (p. 352)		
			aws:TagKeys (p. 352)		comprehend:VolumeKmsKey (p. 352)
			comprehend:ModelKmsKey (p. 352)		comprehend:VpcSecurityGroupIds (p. 352)
			comprehend:VpcSubnets (p. 352)		
DeleteDocumentClassifier	Grants permission to delete a previously created document classifier	Write	document-classifier* (p. 351)		
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* (p. 351)		
			entity-recognizer-endpoint* (p. 351)		
DeleteEntityRecognizer	Grants permission to delete a submitted entity recognizer	Write	entity-recognizer* (p. 351)		
DeleteResourcePolicy	Grants permission to remove policy on resource	Write	document-classifier* (p. 351)		
			entity-recognizer* (p. 351)		
DescribeDocumentClassificationJob	Grants permission to get the properties associated with a document classification job	Read	document-classification-job* (p. 351)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDocumentProperties	Grants permission to get the properties associated with a document classifier	Read	document-classifier* (p. 351)		
DescribeDominantLanguageDetectionJobProperties	Grants permission to get the properties associated with a dominant language detection job	Read	dominant-language-detection-job* (p. 351)		
DescribeEndpointProperties	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* (p. 351)		
			entity-recognizer-endpoint* (p. 351)		
DescribeEntitiesProperties	Grants permission to get the properties associated with an entities detection job	Read	entities-detection-job* (p. 351)		
DescribeEntityRecognizerDetails	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* (p. 351)		
DescribeEventsProperties	Grants permission to get the properties associated with an Events detection job	Read	events-detection-job* (p. 351)		
DescribeKeyPhraseProperties	Grants permission to get the properties associated with a key phrases detection job	Read	key-phrases-detection-job* (p. 351)		
DescribePiiEntityProperties	Grants permission to get the properties associated with a PII entities detection job	Read	pii-entities-detection-job* (p. 351)		
DescribeResourceAttachedPolicies	Grants permission to read attached policy on resource	Read	document-classifier* (p. 351)		
entity-recognizer* (p. 351)					
DescribeSentimentProperties	Grants permission to get the properties associated with a sentiment detection job	Read	sentiment-detection-job* (p. 351)		

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* (p. 350)			
DescribeTopicsDetectionJob	Grants permission to get the properties associated with a topic detection job	Read	topics-detection-job* (p. 351)			
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 (p. 351)			
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				
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				
ImportModel	Grants permission to import a trained Comprehend model	Write	document-classifier* (p. 351)			
			entity-recognizer* (p. 351)			
				aws:RequestTag/\${TagKey} (p. 352)	aws:TagKeys (p. 352)	comprehend:ModelKmsKey (p. 352)
ListDocumentClassificationJobs	Grants permission to get a list of the document classification jobs that you have submitted		Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDocumentClassifiers	Grants permission to get a list of summaries of the document classifiers that you have created	Read			
ListDocumentLabels	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			
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			
ListEntityRecognizers	Grants permission to get a list of summaries for the entity recognizers that you have created	Read			
ListEntityRecognizerProperties	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			
ListKeyPhrasesDetectionJobs	Grants permission to get a list of key phrases 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 (p. 351) document-classifier (p. 351)		

Service Authorization Reference
 Service Authorization Reference
 Amazon Comprehend

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			document-classifier-endpoint (p. 351)		
	dominant-language-detection-job (p. 351)				
	entities-detection-job (p. 351)				
	entity-recognizer (p. 351)				
	entity-recognizer-endpoint (p. 351)				
	events-detection-job (p. 351)				
	key-phrases-detection-job (p. 351)				
	pii-entities-detection-job (p. 351)				
	sentiment-detection-job (p. 351)				
	targeted-sentiment-detection-job (p. 350)				
	ListTargetedSentimentDetectionJobs	Read			
	ListTopicsDetectionJobs	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutResourcePolicy	Grants permission to attach policy to resource	Write	document-classifier* (p. 351)		
	entity-recognizer* (p. 351)				
StartDocumentClassificationJob	Grants permission to start classification job for a document	Write	document-classification-job* (p. 351)		
	document-classifier* (p. 351)		aws:RequestTag/\${TagKey} (p. 352) aws:TagKeys (p. 352)	comprehend:VolumeKmsKey (p. 352) comprehend:OutputKmsKey (p. 352) comprehend:VpcSecurityGroupIds (p. 352) comprehend:VpcSubnets (p. 352)	
StartDominantLanguageDetectionJob	Grants permission to start dominant language detection job for a collection of documents	Write	dominant-language-detection-job* (p. 351)		
			aws:RequestTag/\${TagKey} (p. 352) aws:TagKeys (p. 352)	comprehend:VolumeKmsKey (p. 352) comprehend:OutputKmsKey (p. 352) comprehend:VpcSecurityGroupIds (p. 352) comprehend:VpcSubnets (p. 352)	
StartEntitiesDetectionJob	Grants permission to start asynchronous entity detection job for a collection of documents	Write	entities-detection-job* (p. 351)		
	entity-recognizer (p. 351)				

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					aws:RequestTag/\${TagKey} (p. 352) aws:TagKeys (p. 352) comprehend:VolumeKmsKey (p. 352) comprehend:OutputKmsKey (p. 352) comprehend:VpcSecurityGroupIds (p. 352) comprehend:VpcSubnets (p. 352)
StartEventsDetectionJob	Grants permission to start an asynchronous Events detection job for a collection of documents	Write	events-detection-job* (p. 351)		
					aws:RequestTag/\${TagKey} (p. 352) aws:TagKeys (p. 352) comprehend:OutputKmsKey (p. 352)
StartKeyPhrasesDetectionJob	Grants permission to start an asynchronous key phrase detection job for a collection of documents	Write	key-phrase-detection-job* (p. 351)		
					aws:RequestTag/\${TagKey} (p. 352) aws:TagKeys (p. 352) comprehend:VolumeKmsKey (p. 352) comprehend:OutputKmsKey (p. 352) comprehend:VpcSecurityGroupIds (p. 352) comprehend:VpcSubnets (p. 352)
StartPiiEntitiesDetectionJob	Grants permission to start an asynchronous PII entities detection job for a collection of documents	Write	pii-entities-detection-job* (p. 351)		
					aws:RequestTag/\${TagKey} (p. 352) aws:TagKeys (p. 352) comprehend:OutputKmsKey (p. 352)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartSentimentDetectionJob	Grants permission to start an asynchronous sentiment detection job for a collection of documents	Write	sentiment-detection-job* (p. 351)		
	aws:RequestTag/\${TagKey} (p. 352) aws:TagKeys (p. 352)		comprehend:VolumeKmsKey (p. 352) comprehend:OutputKmsKey (p. 352) comprehend:VpcSecurityGroupIds (p. 352) comprehend:VpcSubnets (p. 352)		
StartTargetedSentimentDetectionJob	Grants permission to start an asynchronous targeted sentiment detection job for a collection of documents	Write	targeted-sentiment-detection-job* (p. 350)		
	aws:RequestTag/\${TagKey} (p. 352) aws:TagKeys (p. 352)		comprehend:VolumeKmsKey (p. 352) comprehend:OutputKmsKey (p. 352) comprehend:VpcSecurityGroupIds (p. 352) comprehend:VpcSubnets (p. 352)		
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* (p. 351)		
	aws:RequestTag/\${TagKey} (p. 352) aws:TagKeys (p. 352)		comprehend:VolumeKmsKey (p. 352) comprehend:OutputKmsKey (p. 352) comprehend:VpcSecurityGroupIds (p. 352) comprehend:VpcSubnets (p. 352)		
StopDominantLanguageDetectionJob	Grants permission to stop a dominant language detection job	Write	dominant-language-detection-job* (p. 351)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopEntitiesDetectionJob	Grants permission to stop an entity detection job	Write	entities-detection-job* (p. 351)		
StopEventsDetectionJob	Grants permission to stop an event detection job	Write	events-detection-job* (p. 351)		
StopKeyPhrasesDetectionJob	Grants permission to stop a key phrase detection job	Write	key-phrases-detection-job* (p. 351)		
StopPiiEntitiesDetectionJob	Grants permission to stop a PII entities detection job	Write	pii-entities-detection-job* (p. 351)		
StopSentimentDetectionJob	Grants permission to stop a sentiment detection job	Write	sentiment-detection-job* (p. 351)		
StopTargetedSentimentDetectionJob	Grants permission to stop a targeted sentiment detection job	Write	targeted-sentiment-detection-job* (p. 350)		
StopTrainingDocumentClassifierJob	Grants permission to stop a previously classified document classifier training job	Write	document-classifier* (p. 351)		
StopTrainingEntityRecognizerJob	Grants permission to stop a previously created entity recognizer training job	Write	entity-recognizer* (p. 351)		
TagResource	Grants permission to tag a resource with given key value pairs	Tagging	document-classification-job (p. 351)		

Service Authorization Reference
 Service Authorization Reference
 Amazon Comprehend

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			entity-recognizer (p. 351)		
			entity-recognizer-endpoint (p. 351)		
			events-detection-job (p. 351)		
			key-phrases-detection-job (p. 351)		
			pii-entities-detection-job (p. 351)		
			sentiment-detection-job (p. 351)		
			topics-detection-job (p. 351)		
				aws:RequestTag/\${TagKey} (p. 352)	
				aws:TagKeys (p. 352)	
UntagResource	Grants permission to untag a resource with given key	Tagging	document-classification-job (p. 351)		
			document-classifier (p. 351)		
			document-classifier-endpoint (p. 351)		
			dominant-language-detection-job (p. 351)		
			entities-detection-job (p. 351)		
			entity-recognizer (p. 351)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			entity-recognizer-endpoint (p. 351)		
			events-detection-job (p. 351)		
			key-phrases-detection-job (p. 351)		
			pii-entities-detection-job (p. 351)		
			sentiment-detection-job (p. 351)		
			topics-detection-job (p. 351)		
				aws:TagKeys (p. 352)	
UpdateEndpoint	Grants permission to update information about the specified endpoint	Write	document-classifier-endpoint* (p. 351)		
	entity-recognizer-endpoint* (p. 351)				

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 \(p. 338\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 352)

Resource types	ARN	Condition keys
document-classifier	arn:\${Partition}:comprehend:\${Region}: \${Account}:document-classifier/ \${DocumentClassifierName}	aws:ResourceTag/ \${TagKey} (p. 352)
document-classifier-endpoint	arn:\${Partition}:comprehend:\${Region}: \${Account}:document-classifier-endpoint/ \${DocumentClassifierEndpointName}	aws:ResourceTag/ \${TagKey} (p. 352)
entity-recognizer	arn:\${Partition}:comprehend:\${Region}: \${Account}:entity-recognizer/ \${EntityRecognizerName}	aws:ResourceTag/ \${TagKey} (p. 352)
entity-recognizer-endpoint	arn:\${Partition}:comprehend:\${Region}: \${Account}:entity-recognizer-endpoint/ \${EntityRecognizerEndpointName}	aws:ResourceTag/ \${TagKey} (p. 352)
dominant-language-detection-job	arn:\${Partition}:comprehend:\${Region}: \${Account}:dominant-language-detection-job/ \${JobId}	aws:ResourceTag/ \${TagKey} (p. 352)
entities-detection-job	arn:\${Partition}:comprehend:\${Region}: \${Account}:entities-detection-job/\${JobId}	aws:ResourceTag/ \${TagKey} (p. 352)
pii-entities-detection-job	arn:\${Partition}:comprehend:\${Region}: \${Account}:pii-entities-detection-job/ \${JobId}	aws:ResourceTag/ \${TagKey} (p. 352)
events-detection-job	arn:\${Partition}:comprehend:\${Region}: \${Account}:events-detection-job/\${JobId}	aws:ResourceTag/ \${TagKey} (p. 352)
key-phrases-detection-job	arn:\${Partition}:comprehend:\${Region}: \${Account}:key-phrases-detection-job/ \${JobId}	aws:ResourceTag/ \${TagKey} (p. 352)
sentiment-detection-job	arn:\${Partition}:comprehend:\${Region}: \${Account}:sentiment-detection-job/\${JobId}	aws:ResourceTag/ \${TagKey} (p. 352)
topics-detection-job	arn:\${Partition}:comprehend:\${Region}: \${Account}:topics-detection-job/\${JobId}	aws:ResourceTag/ \${TagKey} (p. 352)
document-classification-job	arn:\${Partition}:comprehend:\${Region}: \${Account}:document-classification-job/ \${JobId}	aws:ResourceTag/ \${TagKey} (p. 352)

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters access by requiring tag values present in a resource creation request	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters access by requiring tag value associated with the resource	String
<code>aws:TagKeys</code>	Filters access by requiring the presence of mandatory tags in the request	ArrayOfString
<code>comprehend:ModelKmsKey</code>	Filters access by the model KMS key associated with the resource in the request	ARN
<code>comprehend:OutputKmsKey</code>	Filters access by the output KMS key associated with the resource in the request	ARN
<code>comprehend:VolumeKmsKey</code>	Filters access by the volume KMS key associated with the resource in the request	ARN
<code>comprehend:VpcSecurityGroupIdsAssociatedWith</code>	Filters access by the list of all VPC security group ids associated with the resource in the request	ArrayOfString
<code>comprehend:VpcSubnetsAssociatedWith</code>	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 \(p. 352\)](#)
- [Resource types defined by Amazon Comprehend Medical \(p. 355\)](#)
- [Condition keys for Amazon Comprehend Medical \(p. 355\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your

policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeEntities	Grants permission to describe the properties of a medical entity detection job that you have submitted	Read			
DescribeICD10CM	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			
DescribeRxNormLinkingJob	Grants permission to describe the properties of an RxNorm linking job that you have submitted	Read			
DescribeSNOMEDCTLinkingJob	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 information (PHI) entities within the given text document	Read			
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	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Library of Medicine RxNorm database				
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			
ListEntitiesDetectionJobs	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			
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			
StartEntitiesDetectionJobs	Grants permission to start an asynchronous medical entity detection job for a collection of documents	Write			
StartICD10CMInferenceJobs	Grants permission to start an asynchronous ICD-10-CM linking job for a collection of documents	Write			
StartPHIDetectionJobs	Grants permission to start an asynchronous PHI entity detection job for a collection of documents	Write			
StartRxNormInferenceJobs	Grants permission to start an asynchronous RxNorm linking job for a collection of documents	Write			
StartSNOMEDCTInferenceJobs	Grants permission to start an asynchronous SNOMED-CT linking job for a collection of documents	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopEntitiesDetectionJob	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 [Available global condition keys](#).

Condition keys	Description	Type
aws:SourceArn	Filters access by the presence of tag keys in the request	String
aws:SourceVpc	Filters access by the presence of tag keys in the request	String
aws:TagKeys	Filters access by the presence of tag keys in the request	String

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 \(p. 356\)](#)
- [Resource types defined by AWS Compute Optimizer \(p. 357\)](#)
- [Condition keys for AWS Compute Optimizer \(p. 358\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteRecommendations	Grants permission to delete recommendations preferences	Write		compute-optimizer:ResourceType (p. 358)	autoscaling:DescribeAutoScalingGroups ec2:DescribeInstances
DescribeRecommendations	Grants permission to view the status of recommendations export jobs	List			
ExportAutoScalingGroupRecommendations	Grants permission to export Auto Scaling group recommendations to S3 for the provided accounts	Write			autoscaling:DescribeAutoScalingGroups compute-optimizer:GetAutoScalingGroupRecommendations
ExportEBSVolumeRecommendations	Grants permission to export EBS volume recommendations to S3 for the provided accounts	Write			compute-optimizer:GetEBSVolumeRecommendations ec2:DescribeVolumes
ExportEC2InstanceRecommendations	Grants permission to export EC2 instance recommendations to S3 for the provided accounts	Write			compute-optimizer:GetEC2InstanceRecommendations ec2:DescribeInstances
ExportLambdaFunctionRecommendations	Grants permission to export Lambda function recommendations to S3 for the provided accounts	Write			compute-optimizer:GetLambdaFunctionRecommendations lambda>ListFunctions lambda>ListProvisionedConcurrencyConfigurations

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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
GetEC2RecommendationProjectedMetrics	Grants permission to get the recommendationProjectedMetrics of the specified instance	List			ec2:DescribeInstances
GetEffectiveRecommendationPreferences	Grants permission to get recommendationPreferences that are in effect	Read		compute-optimizer:ResourceType (p. 358)	autoscaling:DescribeAutoScalingGroups autoscaling:DescribeAutoScalingInstances ec2:DescribeInstances
GetEnrollmentStatus	Grants permission to get the enrollment status for the specified account	List			
GetOrganizationEnrollmentStatuses	Grants permission to get the enrollment status for member accounts of the organization	List			
GetLambdaFunctionRecommendations	Grants permission to get recommendations for the provided Lambda functions	List			lambda>ListFunctions lambda>ListProvisionedConcurrencyConfigurations
GetRecommendationPreferences	Grants permission to get recommendation preferences	Read		compute-optimizer:ResourceType (p. 358)	
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 (p. 358)	autoscaling:DescribeAutoScalingGroups autoscaling:DescribeAutoScalingInstances ec2:DescribeInstances
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 [Available global condition keys](#).

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

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 \(p. 358\)](#)
- [Resource types defined by AWS Config \(p. 367\)](#)
- [Condition keys for AWS Config \(p. 368\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
<code>BatchGetAggregateConfig</code>	Grants permission to return the current configuration items for	Read	ConfigurationAggregator* (p. 367)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	resources that are present in your AWS Config aggregator				
BatchGetResources	Grants permission to return the 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* (p. 367)		
DeleteConfigRule	Grants permission to delete the specified AWS Config rule and all of its evaluation results	Write	ConfigRule* (p. 367)		
DeleteConfigurationAggregator	Grants permission to delete the specified configuration aggregator and the aggregated data associated with the aggregator	Write	ConfigurationAggregator* (p. 367)		
DeleteConfigurationRecorder	Grants permission to delete the configuration recorder	Write			
DeleteConformancePack	Grants permission to delete the specified conformance pack and all the AWS Config rules and all evaluation results within that conformance pack	Write			
DeleteDeliveryChannel	Grants permission to delete the delivery channel	Write			
DeleteEvaluationResults	Grants permission to delete the evaluation results for the specified Config rule	Write	ConfigRule* (p. 367)		
DeleteOrganizationConfigRule	Grants permission to delete the specified organization config rule and all of its evaluation results from all member accounts in that organization	Write			
DeleteOrganizationConformancePack	Grants permission to delete the specified organization conformance pack and all of its evaluation results from all member accounts in that organization	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeletePendingAuthorizationRequests	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* (p. 367)		
DeleteRemediationExceptions	Grants permission to delete one or more remediation exceptions for specific resource keys for a specific AWS Config Rule	Write			
DeleteResourceConfigurations	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			
DeleteStoredQuery	Grants permission to delete the stored query for an AWS account in an AWS Region	Write	StoredQuery* (p. 368)		
DeliverConfigSnapshot	Grants permission to schedule delivery of a configuration snapshot to the Amazon S3 bucket in the specified delivery channel	Read			
DescribeAggregateComplianceAndNonCompliance	Grants permission to return a list of compliant and noncompliant rules with the number of resources for compliant and noncompliant rules	Read	ConfigurationAggregator* (p. 367)		
DescribeAggregateComplianceAndNoncompliantConformancePacks	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* (p. 367)		
DescribeAggregateAuthorizations	Grants permission to return a list of authorizations granted to various aggregator accounts and regions	List			
DescribeComplianceForConfigRules	Grants permission to indicate whether the specified AWS Config rules are compliant	Read	ConfigRule* (p. 367)		
DescribeComplianceForResources	Grants permission to indicate whether the specified AWS resources are compliant	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeConfigRules	Grants permission to return status information for each of your AWS managed Config rules	Read	ConfigRule* (p. 367)		
DescribeConfigRuleDetails	Grants permission to return details about your AWS Config rules	List	ConfigRule* (p. 367)		
DescribeConfigurationAggregators	Grants permission to return status information for sources within an aggregator	Read	ConfigurationAggregator* (p. 367)		
DescribeConfigurationRecorders	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			
DescribeConfigurationRecorderStatuses	Grants permission to return the names of one or more specified configuration recorders	List			
DescribeConformancePacks	Grants permission to return compliance information for each rule in that conformance pack	Read			
DescribeConformancePackDeploymentStatus	Grants permission to provide one or more performance packs deployment status	Read			
DescribeConformancePacks	Grants permission to return a list of one or more conformance packs	List			
DescribeDeliveryChannel	Grants permission to return the current status of the specified delivery channel	Read			
DescribeDeliveryChannelDetails	Grants permission to return details about the specified delivery channel	List			
DescribeOrganizationConfigRuleDeploymentStatus	Grants permission to provide organization rule configuration 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
DescribeOrganizationConformancePacks	Grants permission to provide pack deployment status for an organization	Read			
DescribeOrganizationPerformancePacks	Grants permission to return a list of organization performance 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* (p. 367)		
DescribeRemediationExceptions	Grants permission to return the details of one or more remediation exceptions	List			
DescribeRemediationExecutionDetails	Grants permission to provide a detailed view of the Remediation Execution for a set of resources including state, timestamps and any error messages for steps that have failed	Read	RemediationConfiguration* (p. 367)		
DescribeRetentionConfigurations	Grants permission to return the details of one or more retention configurations	List			
GetAggregateComplianceForAccounts	Grants permission to return the evaluation results for the specified AWS Config rule for a specific resource in a rule	Read	ConfigurationAggregator* (p. 367)		
GetAggregateComplianceForRegions	Grants permission to return the number of compliant and noncompliant rules for one or more accounts and regions in an aggregator	Read	ConfigurationAggregator* (p. 367)		
GetAggregateComplianceSummary	Grants permission to return the number of compliant and noncompliant conformance packs for one or more accounts and regions in an aggregator	Read	ConfigurationAggregator* (p. 367)		
GetAggregateDiscrepancyCounts	Grants permission to return the resource counts across accounts and regions that are present in your AWS Config aggregator	Read	ConfigurationAggregator* (p. 367)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAggregateResults	Grants permission to return configuration item that is aggregated for your specific resource in a specific source account and region	Read	ConfigurationAggregator* (p. 367)		
GetComplianceDetailsEvaluationResults	Grants permission to return the evaluation results for the specified AWS Config rule	Read	ConfigRule* (p. 367)		
GetComplianceDetailsEvaluationResults	Grants permission to return the evaluation results for the specified AWS resource	Read			
GetComplianceSummaries	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			
GetConformancePackComplianceDetails	Grants permission to return compliance details of a conformance pack for all AWS resources that are monitored by conformance pack	Read			
GetConformancePackComplianceSummary	Grants permission to provide compliance summary for one or more conformance packs	Read			
GetDiscoveredResources	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			
GetOrganizationConfigRuleStatus	Grants permission to return detailed status for each member account within an organization for a given organization config rule	Read			
GetOrganizationConformancePackStatus	Grants permission to return detailed status for each member account within an organization for a given organization conformance pack	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetResourceConfigHistory	Grants permission to return a list of configuration items for the specified resource	Read			
GetStoredQuery	Grants permission to return the details of a specific stored query	Read	StoredQuery* (p. 368)		
ListAggregateDiscoverableResourceTypes	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* (p. 367)		
ListDiscoveredResources	Grants permission to accept a resource type and returns a list of resource identifiers for the resources of that type	List			
ListStoredQueries	Grants permission to list the stored queries for an AWS account in an AWS Region	List	StoredQuery* (p. 368)		
ListTagsForResource	Grants permission to list the tags for AWS Config resource	Read	AggregationAuthorization (p. 367)		
			ConfigRule (p. 367)		
			ConfigurationAggregator (p. 367)		
PutAggregationAuthorization	Grants permission to authorize the aggregator account and region to collect data from the source account and region	Write	AggregationAuthorization* (p. 367)		
			aws:RequestTag/ {\$TagKey} (p. 368)		
			aws:TagKeys (p. 368)		
PutConfigRule	Grants permission to add or update an AWS Config rule for evaluating whether your AWS resources comply with your desired configurations	Write	ConfigRule* (p. 367)		
			aws:RequestTag/ {\$TagKey} (p. 368)		
			aws:TagKeys (p. 368)		
PutConfigurationRecorder	Grants permission to create and update the configuration aggregator with the selected source accounts and regions	Write	ConfigurationAggregator* (p. 367)		
			aws:RequestTag/ {\$TagKey} (p. 368)		
	aws:TagKeys (p. 368)				
PutConfigurationRecorder	Grants permission to create a new configuration recorder to record the selected resource configurations	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutConformancePack	Grants permission to create or update a conformance pack	Write			
PutDeliveryChannel	Grants permission to create a delivery channel object to deliver configuration information to an Amazon S3 bucket and Amazon SNS topic	Write			
PutEvaluations	Grants permission to be used by an AWS Lambda function to deliver evaluation results to AWS Config	Write			
PutExternalEvaluation	Grants permission to deliver an evaluation result to AWS Config	Write			
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			
PutOrganizationConformancePack	Grants permission to add a conformance pack for your entire organization evaluating whether your AWS resources comply with your desired configurations	Write			
PutRemediationConfiguration	Grants permission to add or update the remediation configuration with a specific AWS Config rule with the selected target or action	Write	RemediationConfigurationArn:PassRole		
PutRemediationException	Grants permission to add or update remediation exceptions for specific resources for a specific AWS Config rule	Write			
PutResourceConfig	Grants permission to record the configuration state for the resource provided in the request	Write			
PutRetentionConfig	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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutStoredQuery	Grants permission to save a new query or updates an existing saved query	Write	StoredQuery* (p. 368)		
			aws:RequestTag/ \${TagKey} (p. 368)	aws:TagKeys (p. 368)	
SelectAggregateResourceConfiguredFor	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			
SelectResourceCostConfigured	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* (p. 367)		
StartConfigurationRecording	Grants permission to start recording configurations of the AWS resources you have selected to record in your AWS account	Write			
StartRemediationExecution	Grants permission to run an remediation for the specified AWS Config rules against the last known remediation configuration	Write	RemediationConfiguration (p. 367)	aws:PassRole	
StopConfigurationRecording	Grants permission to stop recording configurations of the AWS resources you have selected to record in your AWS account	Write			
TagResource	Grants permission to associate the specified tags to a resource with the specified resourceArn	Tagging	AggregationAuthorization (p. 367)		
ConfigRule (p. 367)					
ConfigurationAggregator (p. 367)					
ConformancePack (p. 367)					

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 368) aws:TagKeys (p. 368)	
UntagResource	Grants permission to delete specified tags from a resource	Tagging	AggregationAuthorization (p. 367) ConfigRule (p. 367) ConfigurationAggregator (p. 367) ConformancePack (p. 367)		
					aws:TagKeys (p. 368)

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 \(p. 358\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 368)
ConfigurationAggregator	arn:\${Partition}:config:\${Region}: \${Account}:config-aggregator/\${AggregatorId}	aws:ResourceTag/ \${TagKey} (p. 368)
ConfigRule	arn:\${Partition}:config:\${Region}: \${Account}:config-rule/\${ConfigRuleId}	aws:ResourceTag/ \${TagKey} (p. 368)
ConformancePack	arn:\${Partition}:config:\${Region}: \${Account}:conformance-pack/ \${ConformancePackName}/\${ConformancePackId}	aws:ResourceTag/ \${TagKey} (p. 368)
OrganizationConfigRule	arn:\${Partition}:config:\${Region}: \${Account}:organization-config-rule/ \${OrganizationConfigRuleId}	
OrganizationConformancePack	arn:\${Partition}:config:\${Region}: \${Account}:organization-conformance-pack/ \${OrganizationConformancePackId}	
RemediationConfiguration	arn:\${Partition}:config:\${Region}: \${Account}:remediation-configuration/ \${RemediationConfigurationId}	

Resource types	ARN	Condition keys
StoredQuery	arn:\${Partition}:config:\${Region}: \${Account}:stored-query/\${StoredQueryName}/ \${StoredQueryId}	

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 [Available global condition 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 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 \(p. 368\)](#)
- [Resource types defined by Amazon Connect \(p. 393\)](#)
- [Condition keys for Amazon Connect \(p. 394\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateApprovedOrigins	Grants permission to associate approved origin for an existing Amazon Connect instance	Write	instance* (p. 393)		
				connect:InstanceId (p. 395)	
AssociateBot	Grants permission to associate a Lex bot for an existing Amazon Connect instance	Write	instance* (p. 393)		iam:AttachRolePolicy iam>CreateServiceLinkedRole iam:PutRolePolicy lex:CreateResourcePolicy lex:DescribeBotAlias lex:GetBot lex:UpdateResourcePolicy
				connect:InstanceId (p. 395)	
AssociateCustomerProfile	Grants permission to associate a Customer Profile domain for an existing Amazon Connect instance	Write	instance* (p. 393)		iam:AttachRolePolicy iam>CreateServiceLinkedRole iam:PutRolePolicy profile:GetDomain
AssociateDefaultVocabulary	Grants permission to default vocabulary for an existing Amazon Connect instance	Write	instance* (p. 393)		
				connect:InstanceId (p. 395)	
AssociateInstanceStorage	Grants permission to associate Instance Storage for an existing Amazon Connect instance	Write	instance* (p. 393)		ds:DescribeDirectories firehose:DescribeDeliveryStream iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy kinesis:DescribeStream kms:CreateGrant kms:DescribeKey

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					s3:GetBucketAcl s3:GetBucketLocation
			connect:StorageResourceType (p. 395) connect:InstanceId (p. 395)		
AssociateLambdaFunction	Grants permission to associate a Lambda function for an existing Amazon Connect instance	Write	instance* (p. 393)		lambda:AddPermission
			connect:InstanceId (p. 395)		
AssociateLexBot	Grants permission to associate a Lex bot for an existing Amazon Connect instance	Write	instance* (p. 393)		iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy lex:GetBot
			connect:InstanceId (p. 395)		
AssociatePhoneNumberContactFlow	Grants permission to associate contact flow resources to phone number resources in an Amazon Connect instance	Write	contact-flow* (p. 393)		
			phone-number* (p. 394)		
				aws:ResourceTag/ \${TagKey} (p. 395)	connect:InstanceId (p. 395)
AssociateQueueQuickConnect	Grants permission to associate quick connects with a queue in an Amazon Connect instance	Write	queue* (p. 393)		
			quick-connect* (p. 393)		
				aws:ResourceTag/ \${TagKey} (p. 395)	connect:InstanceId (p. 395)
AssociateRoutingProfileQueues	Grants permission to associate queues with a routing profile in an Amazon Connect instance	Write	queue* (p. 393)		
			routing-profile* (p. 393)		
				aws:ResourceTag/ \${TagKey} (p. 395)	connect:InstanceId (p. 395)
AssociateSecurityKey	Grants permission to associate a security key for an existing Amazon Connect instance	Write	instance* (p. 393)		
					connect:InstanceId (p. 395)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchAssociateAnalyticsDataset [permission only]	Grants permission to grant access and to associate the datasets with the specified AWS account	Write	instance* (p. 393)		
BatchDisassociateAnalyticsDataset [permission only]	Grants permission to revoke access and to disassociate the datasets with the specified AWS account	Write	instance* (p. 393)		
ClaimPhoneNumber	Grants permission to claim phone number resources in an Amazon Connect instance	Write	instance* (p. 393) wildcard-phone-number* (p. 394)		
CreateAgentStatus	Grants permission to create agent status in an Amazon Connect instance	Write	agent-status* (p. 394)		
CreateContactFlow	Grants permission to create a contact flow in an Amazon Connect instance	Write	contact-flow* (p. 393)		
CreateContactFlowModule	Grants permission to create a contact flow module in an Amazon Connect instance	Write	contact-flow-module* (p. 394)		
CreateHoursOfOperation	Grants permission to create hours of operation in an Amazon Connect instance	Write	hours-of-operation* (p. 394)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/\${TagKey} (p. 395) aws:TagKeys (p. 395) connect:InstanceId (p. 395)	
CreateInstance	Grants permission to create a new Amazon Connect instance	Write		aws:RequestTag/\${TagKey} (p. 395) aws:TagKeys (p. 395) iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy	
CreateIntegration	Grants permission to create an Integration association with an Amazon Connect instance	Write	instance* (p. 393) integration-association* (p. 394)	app-integrations>CreateEvent connect:DescribeInstance ds:DescribeDirectories events:PutRule events:PutTargets mobiletargeting:GetApp voiceid:DescribeDomain wisdom:GetAssistant wisdom:GetKnowledgeBase	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateQueue	Grants permission to create a queue in an Amazon Connect instance	Write	hours-of-operation* (p. 394) queue* (p. 393) contact-flow (p. 393) phone-number (p. 394) quick-connect (p. 393)		
		Write	quick-connect* (p. 393) contact-flow (p. 393) queue (p. 393) user (p. 393)		
	Grants permission to create a routing profile in an Amazon Connect instance	Write	queue* (p. 393) routing-profile* (p. 393)		
CreateSecurityProfile	Grants permission to create a security profile for the specified Amazon Connect instance	Write	security-profile* (p. 393)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 395) aws:TagKeys (p. 395) connect:InstanceId (p. 395)	
CreateTaskTemplate	Grants permission to create a task template in an Amazon Connect instance	Write	task-template* (p. 393)		
CreateUseCase	Grants permission to create a use case for an integration association	Write	instance* (p. 393) integration-association* (p. 394) use-case* (p. 394)	connect:InstanceId (p. 395) aws:RequestTag/ \${TagKey} (p. 395) aws:TagKeys (p. 395)	connect:DescribeInstances ds:DescribeDirectories
CreateUser	Grants permission to create a user for the specified Amazon Connect instance	Write	routing-profile* (p. 393) security-profile* (p. 393) user* (p. 393) hierarchy-group (p. 393)	aws:RequestTag/ \${TagKey} (p. 395) aws:TagKeys (p. 395) connect:InstanceId (p. 395)	
CreateUserHierarchyGroup	Grants permission to create a user hierarchy group in an Amazon Connect instance	Write	hierarchy-group (p. 393)	aws:RequestTag/ \${TagKey} (p. 395) aws:TagKeys (p. 395) connect:InstanceId (p. 395)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateVocabulary	Grants permission to create a vocabulary in an Amazon Connect instance	Write	vocabulary* (p. 394) 	aws:RequestTag/ \${TagKey} (p. 395) aws:TagKeys (p. 395) connect:InstanceId (p. 395)	
DeleteContactFlow	Grants permission to delete a contact flow in an Amazon Connect instance	Write	contact-flow* (p. 393) 	aws:ResourceTag/ \${TagKey} (p. 395) connect:InstanceId (p. 395)	
DeleteContactFlowModule	Grants permission to delete a contact flow module in an Amazon Connect instance	Write	contact-flow-module* (p. 394) 	aws:ResourceTag/ \${TagKey} (p. 395) connect:InstanceId (p. 395)	
DeleteHoursOfOperation	Grants permission to delete hours of operation in an Amazon Connect instance	Write	hours-of-operation* (p. 394) 	aws:ResourceTag/ \${TagKey} (p. 395) connect:InstanceId (p. 395)	
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* (p. 393) 	ds>DeleteDirectory dsDescribeDirectories dsUnauthorizeApplication	
DeleteIntegration	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* (p. 393) 	app-integrationsDeleteEvent connectDescribeInstance dsDescribeDirectories eventsDeleteRule eventsListTargetsByRule eventsRemoveTargets	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			integration-association* (p. 394)		
				connect:InstanceId (p. 395)	
DeleteQuickConnect	Grants permission to delete a quick connect in an Amazon Connect instance	Write	quick-connect* (p. 393)		
				aws:ResourceTag/\${TagKey} (p. 395)	
				connect:InstanceId (p. 395)	
DeleteSecurityProfile	Grants permission to delete a security profile in an Amazon Connect instance	Write	security-profile* (p. 393)		
				aws:ResourceTag/\${TagKey} (p. 395)	
				connect:InstanceId (p. 395)	
DeleteTaskTemplate	Grants permission to delete a task template in an Amazon Connect instance	Write	task-template* (p. 393)		
				aws:ResourceTag/\${TagKey} (p. 395)	
				connect:InstanceId (p. 395)	
DeleteUseCase	Grants permission to delete a use case from an integration association	Write	instance* (p. 393)		connect:DescribeInstances ds:DescribeDirectories
			use-case* (p. 394)		
				connect:InstanceId (p. 395)	
DeleteUser	Grants permission to delete a user in an Amazon Connect instance	Write	user* (p. 393)		
				aws:ResourceTag/\${TagKey} (p. 395)	
				connect:InstanceId (p. 395)	
DeleteUserHierarchyGroup	Grants permission to delete a user hierarchy group in an Amazon Connect instance	Write	hierarchy-group* (p. 393)		
				connect:InstanceId (p. 395)	
DeleteVocabulary	Grants permission to delete a vocabulary in an Amazon Connect instance	Write	vocabulary* (p. 394)		
				aws:ResourceTag/\${TagKey} (p. 395)	
				connect:InstanceId (p. 395)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeAgentStatus	Grants permission to describe agent status in an Amazon Connect instance	Read	agent-status* (p. 394)		
			aws:ResourceTag/\${TagKey} (p. 395)	connect:InstanceId (p. 395)	
DescribeContact	Grants permission to describe a contact in an Amazon Connect instance	Read	contact* (p. 393)		
			connect:InstanceId (p. 395)		
DescribeContactFlow	Grants permission to describe a contact flow in an Amazon Connect instance	Read	contact-flow* (p. 393)		
			aws:ResourceTag/\${TagKey} (p. 395)	connect:InstanceId (p. 395)	
DescribeContactFlowModule	Grants permission to describe a contact flow module in an Amazon Connect instance	Read	contact-flow-module* (p. 394)		
			aws:ResourceTag/\${TagKey} (p. 395)	connect:InstanceId (p. 395)	
DescribeHoursOfOperation	Grants permission to describe hours of operation in an Amazon Connect instance	Read	hours-of-operation* (p. 394)		
			aws:ResourceTag/\${TagKey} (p. 395)	connect:InstanceId (p. 395)	
DescribeInstance	Grants permission to view details of an Amazon Connect instance and is also required to create an instance	Read	instance* (p. 393)	ds:DescribeDirectories	
			connect:InstanceId (p. 395)	aws:ResourceTag/\${TagKey} (p. 395)	
DescribeInstanceAttribute	Grants permission to view the attribute details of an existing Amazon Connect instance	Read	instance* (p. 393)		
			connect:AttributeType (p. 395)	connect:InstanceId (p. 395)	
DescribeInstanceStateStorage	Grants permission to view the storage configuration for an existing Amazon Connect instance	Read	instance* (p. 393)		
			connect:StorageResourceType (p. 395)	connect:InstanceId (p. 395)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribePhoneNumber	Grants permission to describe phone number resources in an Amazon Connect instance	List	phone-number* (p. 394)		
			aws:ResourceTag/\${TagKey} (p. 395)		
DescribeQueue	Grants permission to describe a queue in an Amazon Connect instance	Read	queue* (p. 393)		
			aws:ResourceTag/\${TagKey} (p. 395)		
			connect:InstanceId (p. 395)		
DescribeQuickConnect	Grants permission to describe quick connect in an Amazon Connect instance	Read	quick-connect* (p. 393)		
			aws:ResourceTag/\${TagKey} (p. 395)		
			connect:InstanceId (p. 395)		
DescribeRoutingProfile	Grants permission to describe routing profile in an Amazon Connect instance	Read	routing-profile* (p. 393)		
			aws:ResourceTag/\${TagKey} (p. 395)		
			connect:InstanceId (p. 395)		
DescribeSecurityProfile	Grants permission to describe security profile in an Amazon Connect instance	Read	security-profile* (p. 393)		
			aws:ResourceTag/\${TagKey} (p. 395)		
			connect:InstanceId (p. 395)		
DescribeUser	Grants permission to describe a user in an Amazon Connect instance	Read	user* (p. 393)		
			aws:ResourceTag/\${TagKey} (p. 395)		
			connect:InstanceId (p. 395)		
DescribeUserHierarchyGroup	Grants permission to describe a hierarchy group for an Amazon Connect instance	Read	hierarchy-group* (p. 393)		
			connect:InstanceId (p. 395)		
DescribeUserHierarchyStructure	Grants permission to describe the hierarchy structure for an Amazon Connect instance	Read	instance* (p. 393)		
			connect:InstanceId (p. 395)		
DescribeVocabulary	Grants permission to describe vocabulary in an Amazon Connect instance	Read	vocabulary* (p. 394)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/ \${TagKey} (p. 395) connect:InstanceId (p. 395)	
DisassociateApprovedOrigin	Grants permission to disassociate approved origin for an existing Amazon Connect instance	Write	instance* (p. 393)		
				connect:InstanceId (p. 395)	
DisassociateBot	Grants permission to disassociate a Lex bot for an existing Amazon Connect instance	Write	instance* (p. 393)		iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy lex:DeleteResourcePolicy lex:UpdateResourcePolicy
				connect:InstanceId (p. 395)	
DisassociateCustomerProfile	Grants permission to disassociate Customer Profiles domain for an existing Amazon Connect instance	Write	instance* (p. 393)		iam:AttachRolePolicy iam:DeleteRolePolicy iam:DetachRolePolicy iam:GetPolicy iam:GetPolicyVersion iam:GetRolePolicy
				connect:StorageResourceType (p. 395)	
DisassociateInstanceStorage	Grants permission to disassociate instance storage for an existing Amazon Connect instance	Write	instance* (p. 393)		connect:InstanceId (p. 395)
				connect:StorageResourceType (p. 395)	
DisassociateLambdaFunction	Grants permission to disassociate a Lambda function for an existing Amazon Connect instance	Write	instance* (p. 393)		lambda:RemovePermission
				connect:InstanceId (p. 395)	
DisassociateLexBot	Grants permission to disassociate a Lex bot for an existing Amazon Connect instance	Write	instance* (p. 393)		iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy
				connect:InstanceId (p. 395)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociatePhoneNumberFromContactFlow	Grants permission to disassociate contact flow resources from phone number resources in an Amazon Connect instance	Write	phone-number* (p. 394) aws:ResourceTag/ {\$TagKey} (p. 395)		
DisassociateQuickConnects	Grants permission to disassociate quick connects from a queue in an Amazon Connect instance	Write	queue* (p. 393) quick-connect* (p. 393) aws:ResourceTag/ {\$TagKey} (p. 395)		connect:InstanceId (p. 395)
DisassociateRoutingProfileQueues	Grants permission to disassociate queues from a routing profile in an Amazon Connect instance	Write	routing-profile* (p. 393) aws:ResourceTag/ {\$TagKey} (p. 395)		connect:InstanceId (p. 395)
DisassociateSecurityKey	Grants permission to disassociate the security key for an existing Amazon Connect instance	Write	instance* (p. 393) connect:InstanceId (p. 395)		
GetContactAttributes	Grants permission to retrieve the contact attributes for the specified contact	Read	contact* (p. 393) connect:InstanceId (p. 395)		
GetCurrentMetricData	Grants permission to retrieve current metric data for the queues in an Amazon Connect instance	Read	queue* (p. 393) connect:InstanceId (p. 395)		
GetFederationToken	Grants permission to federate into an Amazon Connect instance when using SAML-based authentication for identity management	Read	instance* (p. 393) connect:InstanceId (p. 395)		
GetFederationTokenForEmergencyAccess	Grants permission to federate into an Amazon Connect instance (Log in for emergency access functionality in the Amazon Connect console)	Write	instance* (p. 393)		connect:DescribeInstances connect:ListInstances ds:DescribeDirectories
GetMetricData	Grants permission to retrieve historical metric data for queues in an Amazon Connect instance	Read	queue* (p. 393) connect:InstanceId (p. 395)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTaskTemplate	Grants permission to get details about specified task template in an Amazon Connect instance	Read	task-template* (p. 393)		
				aws:ResourceTag/\${TagKey} (p. 395)	connect:InstanceId (p. 395)
ListAgentStatuses	Grants permission to list agent statuses in an Amazon Connect instance	List	wildcard-agent-status* (p. 394)		
ListApprovedOrigins	Grants permission to view approved origins of an existing Amazon Connect instance	List	instance* (p. 393)		connect:InstanceId (p. 395)
ListBots	Grants permission to view the Lex bots of an existing Amazon Connect instance	List	instance* (p. 393)		connect:InstanceId (p. 395)
ListContactFlowModules	Grants permission to list contact flow module resources in an Amazon Connect instance	List	instance* (p. 393)		
ListContactFlows	Grants permission to list contact flow resources in an Amazon Connect instance	List	wildcard-contact-flow* (p. 394)		
ListContactReferences	Grants permission to list references associated with a contact in an Amazon Connect instance	List	contact* (p. 393)		connect:InstanceId (p. 395)
ListDefaultVocabularies	Grants permission to list default vocabularies associated with a Amazon Connect instance	List	instance* (p. 393)		connect:InstanceId (p. 395)
ListHoursOfOperation	Grants permission to list hours of operation resources in an Amazon Connect instance	List	instance* (p. 393)		connect:InstanceId (p. 395)
ListInstanceAttributes	Grants permission to view the attributes of an existing Amazon Connect instance	List	instance* (p. 393)		connect:InstanceId (p. 395)
ListInstanceStorageConfigurations	Grants permission to view storage configurations of an existing Amazon Connect instance	List	instance* (p. 393)		connect:InstanceId (p. 395)
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* (p. 393)		connect:DescribeInstances ds:DescribeDirectories
	connect:InstanceId (p. 395)				
ListLambdaFunctions	Grants permission to view the Lambda functions of an existing Amazon Connect instance	List	instance* (p. 393)		connect:InstanceId (p. 395)
	connect:InstanceId (p. 395)				
ListLexBots	Grants permission to view the Lex bots of an existing Amazon Connect instance	List	instance* (p. 393)		connect:InstanceId (p. 395)
	connect:InstanceId (p. 395)				
ListPhoneNumbers	Grants permission to list phone number resources in an Amazon Connect instance	List	wildcard-legacy-phone-number* (p. 394)		
ListPhoneNumberNumbers	Grants permission to list phone number resources in an Amazon Connect instance	List	wildcard-phone-number* (p. 394)		
	connect:InstanceId (p. 395)				
ListPrompts	Grants permission to list prompt resources in an Amazon Connect instance	List	instance* (p. 393)		connect:InstanceId (p. 395)
	connect:InstanceId (p. 395)				
ListQueueQuickConnects	Grants permission to list quick connect resources in a queue in an Amazon Connect instance	List	queue* (p. 393)		
	aws:ResourceTag/ \${TagKey} (p. 395)		connect:InstanceId (p. 395)		
ListQueues	Grants permission to list queue resources in an Amazon Connect instance	List	wildcard-queue* (p. 393)		
ListQuickConnects	Grants permission to list quick connect resources in an Amazon Connect instance	List	wildcard-quick-connect* (p. 393)		
ListRealtimeContactAnalysisSegments	Grants permission to list the contact analysis segments for a real-time analysis session	Read	contact* (p. 393)		
ListRoutingProfileResources	Grants permission to list queue resources in a routing profile in an Amazon Connect instance	List	routing-profile* (p. 393)		
	aws:ResourceTag/ \${TagKey} (p. 395)		connect:InstanceId (p. 395)		
ListRoutingProfiles		List	instance* (p. 393)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to list routing profile resources in an Amazon Connect instance				connect:InstanceId (p. 395)
ListSecurityKeys	Grants permission to view the security keys of an existing Amazon Connect instance	List	instance* (p. 393)		
					connect:InstanceId (p. 395)
ListSecurityProfilePermissions	Grants permission to list permissions associated with security profile in an Amazon Connect instance	List	security-profile* (p. 393)		
					aws:ResourceTag/\${TagKey} (p. 395) connect:InstanceId (p. 395)
ListSecurityProfiles	Grants permission to list security profile resources in an Amazon Connect instance	List	instance* (p. 393)		
					connect:InstanceId (p. 395)
ListTagsForResource	Grants permission to list tags for an Amazon Connect resource	Read	agent-status (p. 394)		
			contact-flow (p. 393)		
			contact-flow-module (p. 394)		
			hierarchy-group (p. 393)		
			hours-of-operation (p. 394)		
			integration-association (p. 394)		
			phone-number (p. 394)		
			queue (p. 393)		
			quick-connect (p. 393)		
			routing-profile (p. 393)		
			security-profile (p. 393)		
			use-case (p. 394)		
			user (p. 393)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			wildcard-phone-number (p. 394)		
			aws:ResourceTag/\${TagKey} (p. 395)		
ListTaskTemplate	Grants permission to list task template resources in an Amazon Connect instance	List	instance* (p. 393)		
ListUseCases	Grants permission to list the use cases of an integration association	List	instance* (p. 393)		connect:DescribeInstance
				ds:DescribeDirectories	
ListUserHierarchy	Grants permission to list the hierarchy group resources in an Amazon Connect instance	List	instance* (p. 393)		
				connect:InstanceId (p. 395)	
ListUsers	Grants permission to list user resources in an Amazon Connect instance	List	instance* (p. 393)		
				connect:InstanceId (p. 395)	
PutUserStatus	Grants permission to switch User Status in an Amazon Connect instance	Write	agent-status* (p. 394)		
	instance* (p. 393)				
	user* (p. 393)				
	aws:ResourceTag/\${TagKey} (p. 395)				
				connect:InstanceId (p. 395)	
ReleasePhoneNumber	Grants permission to release phone number resources in an Amazon Connect instance	Write	phone-number* (p. 394)		
	aws:ResourceTag/\${TagKey} (p. 395)				
ResumeContactRecording	Grants permission to resume recording for the specified contact	Write	contact* (p. 393)		
SearchAvailablePhoneNumbers	Grants permission to search phone number resources in an Amazon Connect instance	List	wildcard-phone-number* (p. 394)		
SearchUsers	Grants permission to search user resources in an Amazon Connect instance	Read	instance* (p. 393)		connect:DescribeUser
	connect:InstanceId (p. 395)				
	connect:SearchTag/\${TagKey} (p. 395)				

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SearchVocabularies	Grants permission to search vocabularies in a Amazon Connect instance	List	vocabulary* (p. 394)		
	connect:InstanceId (p. 395)				
StartChatContact	Grants permission to initiate a chat using the Amazon Connect API	Write	contact-flow* (p. 393)		
StartContactRecording	Grants permission to start recording for the specified contact	Write	contact* (p. 393)		
StartContactStreaming	Grants permission to start chat streaming using the Amazon Connect API	Write	instance* (p. 393)		
StartOutboundVoiceCalls	Grants permission to initiate outbound calls using the Amazon Connect API	Write	contact* (p. 393)		
StartTaskContact	Grants permission to initiate a task using the Amazon Connect API	Write	contact-flow* (p. 393)		
connect:InstanceId (p. 395)					
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* (p. 393)		
connect:InstanceId (p. 395)					
StopContactRecording	Grants permission to stop recording for the specified contact	Write	contact* (p. 393)		
StopContactStreaming	Grants permission to stop chat streaming using the Amazon Connect API	Write	instance* (p. 393)		
SuspendContactRecording	Grants permission to suspend recording for the specified contact	Write	contact* (p. 393)		
TagResource	Grants permission to tag an Amazon Connect resource	Tagging	agent-status (p. 394)		
contact-flow (p. 393)					
contact-flow-module (p. 394)					

Service Authorization Reference
Service Authorization Reference
Amazon Connect

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			hierarchy-group (p. 393) hours-of-operation (p. 394) integration-association (p. 394) phone-number (p. 394) queue (p. 393) quick-connect (p. 393) routing-profile (p. 393) security-profile (p. 393) use-case (p. 394) user (p. 393) wildcard-phone-number (p. 394) aws:TagKeys (p. 395) aws:RequestTag/\${TagKey} (p. 395)		
TransferContact	Grants permission to transfer the contact to another queue or agent	Write	contact* (p. 393)		
contact-flow* (p. 393)					
instance* (p. 393)					
connect:InstanceId (p. 395)					
UntagResource	Grants permission to untag an Amazon Connect resource	Tagging	agent-status (p. 394)		
contact-flow (p. 393)					
contact-flow-module (p. 394)					

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			hierarchy-group (p. 393) hours-of-operation (p. 394) integration-association (p. 394) phone-number (p. 394) queue (p. 393) quick-connect (p. 393) routing-profile (p. 393) security-profile (p. 393) use-case (p. 394) user (p. 393) wildcard-phone-number (p. 394)		
	Grants permission to update agent status in an Amazon Connect instance	Write	agent-status* (p. 394)		
			aws:ResourceTag/\${TagKey} (p. 395)	connect:InstanceId (p. 395)	
	Grants permission to update a contact in an Amazon Connect instance	Write	contact* (p. 393)		
				connect:InstanceId (p. 395)	
	Grants permission to create or update the contact attributes associated with the specified contact	Write	contact* (p. 393)		
				connect:InstanceId (p. 395)	
	Grants permission to update contact flow content in an Amazon Connect instance	Write	contact-flow* (p. 393)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/ \${TagKey} (p. 395) connect:InstanceId (p. 395)	
UpdateContactFlowMetadata	Grants permission to update the Metadata of a contact flow in an Amazon Connect instance	Write	contact-flow* (p. 393)		
			aws:ResourceTag/ \${TagKey} (p. 395) connect:InstanceId (p. 395)		
UpdateContactFlowModuleContent	Grants permission to update contact flow module content in an Amazon Connect instance	Write	contact-flow-module* (p. 394)		
			aws:ResourceTag/ \${TagKey} (p. 395) connect:InstanceId (p. 395)		
UpdateContactFlowModuleMetadata	Grants permission to update the Metadata of a contact flow module in an Amazon Connect instance	Write	contact-flow-module* (p. 394)		
			aws:ResourceTag/ \${TagKey} (p. 395) connect:InstanceId (p. 395)		
UpdateContactFlowName	Grants permission to update the name and description of a contact flow in an Amazon Connect instance	Write	contact-flow* (p. 393)		
			aws:ResourceTag/ \${TagKey} (p. 395) connect:InstanceId (p. 395)		
UpdateContactSchedule	Grants permission to update the schedule of a contact that is already scheduled in an Amazon Connect instance	Write	contact* (p. 393)		
				connect:InstanceId (p. 395)	
UpdateHoursOfOperation	Grants permission to update the hours of operation in an Amazon Connect instance	Write	hours-of-operation* (p. 394)		
			aws:ResourceTag/ \${TagKey} (p. 395) connect:InstanceId (p. 395)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateInstanceAttribute	Grants permission to update the attribute for an existing Amazon Connect instance	Write	instance* (p. 393)		ds:DescribeDirectories iam:AttachRolePolicy iam>CreateServiceLinkedRole iam:PutRolePolicy logs>CreateLogGroup
					connect:AttributeType (p. 395) connect:InstanceId (p. 395)
UpdateInstanceStorageConfiguration	Grants permission to update the storage configuration for an existing Amazon Connect instance	Write	instance* (p. 393)		ds:DescribeDirectories firehose:DescribeDeliveryStream iam:AttachRolePolicy iam>CreateServiceLinkedRole iam:PutRolePolicy kinesis:DescribeStream kms>CreateGrant kms:DescribeKey s3:GetBucketAcl s3:GetBucketLocation
					connect:StorageResourceType (p. 395) connect:InstanceId (p. 395)
UpdatePhoneNumber	Grants permission to update phone number resources in an Amazon Connect instance	Write	instance* (p. 393)		
			phone-number* (p. 394)		
					aws:ResourceTag/\${TagKey} (p. 395)
UpdateQueueHoursOfOperation	Grants permission to update queue hours of operation in an Amazon Connect instance	Write	hours-of-operation* (p. 394)		
			queue* (p. 393)		
					aws:ResourceTag/\${TagKey} (p. 395) connect:InstanceId (p. 395)
UpdateQueueMaxContacts		Write	queue* (p. 393)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to update queue capacity in an Amazon Connect instance			aws:ResourceTag/ \${TagKey} (p. 395) connect:InstanceId (p. 395)	
UpdateQueueName	Grants permission to update a queue name and description in an Amazon Connect instance	Write	queue* (p. 393)		
				aws:ResourceTag/ \${TagKey} (p. 395) connect:InstanceId (p. 395)	
UpdateQueueOutboundCallerConfig	Grants permission to update queue outbound caller config in an Amazon Connect instance	Write	queue* (p. 393)		
			contact-flow (p. 393)		
UpdateQueueStatus	Grants permission to update queue status in an Amazon Connect instance	Write	phone-number (p. 394)		
				aws:ResourceTag/ \${TagKey} (p. 395) connect:InstanceId (p. 395)	
UpdateQuickConnectConfiguration	Grants permission to update the configuration of a quick connect in an Amazon Connect instance	Write	queue* (p. 393)		
				aws:ResourceTag/ \${TagKey} (p. 395) connect:InstanceId (p. 395)	
UpdateQuickConnectName	Grants permission to update a quick connect name and description in an Amazon Connect instance	Write	quick-connect* (p. 393)		
			contact-flow (p. 393)		
UpdateQuickConnectDescription	Grants permission to update a quick connect description in an Amazon Connect instance	Write	queue (p. 393)		
			user (p. 393)		
UpdateQuickConnectArn	Grants permission to update a quick connect ARN in an Amazon Connect instance	Write		aws:ResourceTag/ \${TagKey} (p. 395) connect:InstanceId (p. 395)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateRoutingProfile	Grants permission to update the connect:currency /routing profile in an Amazon Connect instance	Write	routing-profile* (p. 393)		
				aws:ResourceTag/ {\$TagKey} (p. 395)	connect:InstanceId (p. 395)
UpdateRoutingProfileDefaultQueueInRouting	Grants permission to update the profile:queue routing profile in an Amazon Connect instance	Write	queue* (p. 393)		
			routing-profile* (p. 393)		
				aws:ResourceTag/ {\$TagKey} (p. 395)	
				connect:InstanceId (p. 395)	
UpdateRoutingProfileQueue	Grants permission to update the queue:queue routing profile in an Amazon Connect instance	Write	routing-profile* (p. 393)		
				aws:ResourceTag/ {\$TagKey} (p. 395)	
				connect:InstanceId (p. 395)	
UpdateSecurityProfile	Grants permission to update a security:profile security profile group for a user in an Amazon Connect instance	Write	security-profile* (p. 393)		
				aws:ResourceTag/ {\$TagKey} (p. 395)	
				connect:InstanceId (p. 395)	
UpdateTaskTemplate	Grants permission to update a task:template task template belonging to a Amazon Connect instance	Write	task-template* (p. 393)		
				aws:ResourceTag/ {\$TagKey} (p. 395)	
				connect:InstanceId (p. 395)	
UpdateUserHierarchyGroup	Grants permission to update a hierarchy:group hierarchy group for a user in an Amazon Connect instance	Write	user* (p. 393)		
			hierarchy-group (p. 393)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/ \${TagKey} (p. 395) connect:InstanceId (p. 395)	
UpdateUserHierarchyGroup	Grants permission to update a <code>userHierarchyGroup</code> name in an Amazon Connect instance	Write	hierarchy-group* (p. 393)		
				connect:InstanceId (p. 395)	
UpdateUserHierarchyStructure	Grants permission to update <code>userHierarchy</code> structure in an Amazon Connect instance	Write	instance* (p. 393)		
				connect:InstanceId (p. 395)	
UpdateUserIdentity	Grants permission to update <code>identity</code> information for a user in an Amazon Connect instance	Write	user* (p. 393)		
				aws:ResourceTag/ \${TagKey} (p. 395) connect:InstanceId (p. 395)	
UpdateUserPhoneConfig	Grants permission to update <code>phoneConfig</code> configuration settings for a user in an Amazon Connect instance	Write	user* (p. 393)		
				aws:ResourceTag/ \${TagKey} (p. 395) connect:InstanceId (p. 395)	
UpdateUserRoutingProfile	Grants permission to update a <code>routingProfile</code> profile for a user in an Amazon Connect instance	Write	routing-profile* (p. 393)		
				aws:ResourceTag/ \${TagKey} (p. 395) connect:InstanceId (p. 395)	
UpdateUserSecurityProfile	Grants permission to update <code>securityProfile</code> profiles for a user in an Amazon Connect instance	Write	security-profile* (p. 393)		
				aws:ResourceTag/ \${TagKey} (p. 395) connect:InstanceId (p. 395)	
UpdatedescribeContactFlow	Grants permission to update <code>contactFlow</code> module content in an Amazon Connect instance	Write	contact-flow-module* (p. 394)		
				aws:ResourceTag/ \${TagKey} (p. 395) connect:InstanceId (p. 395)	

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 \(p. 368\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 395)
contact	arn:\${Partition}:connect:\${Region}: \${Account}:instance/\${InstanceId}/contact/ \${ContactId}	
user	arn:\${Partition}:connect:\${Region}: \${Account}:instance/\${InstanceId}/agent/ \${UserId}	aws:ResourceTag/\${TagKey} (p. 395)
routing-profile	arn:\${Partition}:connect:\${Region}: \${Account}:instance/\${InstanceId}/routing-profile/\${RoutingProfileId}	aws:ResourceTag/\${TagKey} (p. 395)
security-profile	arn:\${Partition}:connect:\${Region}: \${Account}:instance/\${InstanceId}/security-profile/\${SecurityProfileId}	aws:ResourceTag/\${TagKey} (p. 395)
hierarchy-group	arn:\${Partition}:connect:\${Region}: \${Account}:instance/\${InstanceId}/agent-group/\${HierarchyGroupId}	aws:ResourceTag/\${TagKey} (p. 395)
queue	arn:\${Partition}:connect:\${Region}: \${Account}:instance/\${InstanceId}/queue/ \${QueueId}	aws:ResourceTag/\${TagKey} (p. 395)
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} (p. 395)
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} (p. 395)
task-template	arn:\${Partition}:connect:\${Region}: \${Account}:instance/\${InstanceId}/task-template/\${TaskTemplateId}	aws:ResourceTag/\${TagKey} (p. 395)

Resource types	ARN	Condition keys
contact-flow-module	arn:\${Partition}:connect:\${Region}: \${Account}:instance/\${InstanceId}/flow-module/\${ContactFlowModuleId}	aws:ResourceTag/\${TagKey} (p. 395)
wildcard-contact-flow	arn:\${Partition}:connect:\${Region}: \${Account}:instance/\${InstanceId}/contact-flow/*	
hours-of-operation	arn:\${Partition}:connect:\${Region}: \${Account}:instance/\${InstanceId}/operating-hours/\${HoursOfOperationId}	aws:ResourceTag/\${TagKey} (p. 395)
agent-status	arn:\${Partition}:connect:\${Region}: \${Account}:instance/\${InstanceId}/agent-state/\${AgentStatusId}	aws:ResourceTag/\${TagKey} (p. 395)
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} (p. 395)
wildcard-phone-number	arn:\${Partition}:connect:\${Region}: \${Account}:phone-number/*	aws:ResourceTag/\${TagKey} (p. 395)
integration-association	arn:\${Partition}:connect: \${Region}: \${Account}:instance/ \${InstanceId}/integration-association/ \${IntegrationAssociationId}	aws:ResourceTag/\${TagKey} (p. 395)
use-case	arn:\${Partition}:connect:\${Region}: \${Account}:instance/\${InstanceId}/use-case/\${UseCaseId}	aws:ResourceTag/\${TagKey} (p. 395)
vocabulary	arn:\${Partition}:connect:\${Region}: \${Account}:instance/\${InstanceId}/vocabulary/\${VocabularyId}	aws:ResourceTag/\${TagKey} (p. 395)

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 [Available global condition 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:AttributeType	Filters access by the attribute type of the Amazon Connect instance	String
connect:InstanceId	Filters access by restricting federation into specified Amazon Connect instances	String
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

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 \(p. 395\)](#)
- [Resource types defined by Amazon Connect Customer Profiles \(p. 398\)](#)
- [Condition keys for Amazon Connect Customer Profiles \(p. 399\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 399)		
CreateDomain	Grants permission to create a Domain	Write		aws:RequestTag/\${TagKey} (p. 399) aws:TagKeys (p. 399)	
CreateIntegrationWorkflow	Grants permission to create an integration workflow in a domain	Write	domains* (p. 399)		
				aws:RequestTag/\${TagKey} (p. 399) aws:TagKeys (p. 399)	
CreateProfile	Grants permission to create a profile in the domain	Write	domains* (p. 399)		
DeleteDomain	Grants permission to delete a Domain	Write	domains* (p. 399)		
DeleteIntegration	Grants permission to delete an integration in a domain	Write	domains* (p. 399)		
				integrations* (p. 399)	
DeleteProfile	Grants permission to delete a profile	Write	domains* (p. 399)		
DeleteProfileKey	Grants permission to delete a profile key	Write	domains* (p. 399)		
DeleteProfileObject	Grants permission to delete a profile object	Write	domains* (p. 399)		
				object-types* (p. 399)	
DeleteProfileObjectType	Grants permission to delete a specific profile object type in the domain	Write	domains* (p. 399)		
				object-types* (p. 399)	
DeleteWorkflow	Grants permission to delete a workflow in a domain	Write	domains* (p. 399)		
GetAutoMergingPreview	Grants permission to get a preview of auto merging in a domain	Read	domains* (p. 399)		
GetDomain	Grants permission to get a specific domain in an account	Read	domains* (p. 399)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetIdentityResolutionJobs	Grants permission to get an identity resolution job in a domain	Read	domains* (p. 399)		
GetIntegrations	Grants permission to get a specific integrations in a domain	Read	domains* (p. 399)		
			integrations* (p. 399)		
GetMatches	Grants permission to get profile matches in a domain	List	domains* (p. 399)		
GetProfileObjectTypes	Grants permission to get a specific profile object type in the domain	Read	domains* (p. 399)		
			object-types* (p. 399)		
GetProfileObjectTemplate	Grants permission to get a specific object type template	Read			
GetWorkflow	Grants permission to get workflow details in a domain	Read	domains* (p. 399)		
GetWorkflowStep	Grants permission to get workflow step details in a domain	Read	domains* (p. 399)		
ListAccountIntegrations	Grants permission to list all the integrations in the account	List			
ListDomains	Grants permission to list all the domains in an account	List			
ListIdentityResolutionJobs	Grants permission to list identity resolution jobs in a domain	List	domains* (p. 399)		
ListIntegrations	Grants permission to list all the integrations in a specific domain	List	domains* (p. 399)		
ListProfileObjectTypes	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* (p. 399)		
ListProfileObjects	Grants permission to list all the profile objects for a profile	List	domains* (p. 399)		
object-types* (p. 399)					
ListTagsForResource	Grants permission to list tags for a resource	Read			
ListWorkflows	Grants permission to list all the workflows in a specific domain	List	domains* (p. 399)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
MergeProfiles	Grants permission to merge profiles in a domain	Write	domains* (p. 399)		
PutIntegration	Grants permission to put a integration in a domain	Write	domains* (p. 399)		
			integrations* (p. 399)		
			aws:RequestTag/\${TagKey} (p. 399)		
PutProfileObject	Grants permission to put an object for a profile	Write	domains* (p. 399)		
PutProfileObjectType	Grants permission to put a specific profile object type in the domain	Write	domains* (p. 399)		
			object-types* (p. 399)		
			aws:RequestTag/\${TagKey} (p. 399)		
SearchProfiles	Grants permission to search for profiles in a domain	Read	domains* (p. 399)		
TagResource	Grants permission to adds tags to a resource	Tagging		aws:RequestTag/\${TagKey} (p. 399)	
			aws:TagKeys (p. 399)		
UntagResource	Grants permission to remove tags from a resource	Tagging		aws:RequestTag/\${TagKey} (p. 399)	
			aws:TagKeys (p. 399)		
UpdateDomain	Grants permission to update a Domain	Write	domains* (p. 399)		
UpdateProfile	Grants permission to update a profile in the domain	Write	domains* (p. 399)		

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 \(p. 395\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 399)
object-types	arn:\${Partition}:profile:\${Region}: \${Account}:domains/\${DomainName}/object-types/\${ObjectName}	aws:ResourceTag/ \${TagKey} (p. 399)
integrations	arn:\${Partition}:profile:\${Region}: \${Account}:domains/\${DomainName}/integrations/\${Uri}	aws:ResourceTag/ \${TagKey} (p. 399)

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 [Available global condition 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 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 \(p. 400\)](#)
- [Resource types defined by Amazon Connect Voice ID \(p. 401\)](#)
- [Condition keys for Amazon Connect Voice ID \(p. 402\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDomain	Grants permission to create a domain	Write		aws:RequestTag/\${TagKey} (p. 402) aws:TagKeys (p. 402)	
DeleteDomain	Grants permission to delete a domain	Write	domain* (p. 402)		
DeleteFraudster	Grants permission to delete a fraudster	Write	domain* (p. 402)		
DeleteSpeaker	Grants permission to delete a speaker	Write	domain* (p. 402)		
DescribeComplianceConsent [permission only]	Grants permission to describe compliance consent	Read			
DescribeDomain	Grants permission to describe a domain	Read	domain* (p. 402)		
DescribeFraudster	Grants permission to describe a fraudster	Read	domain* (p. 402)		
DescribeFraudsterRegistrationJob	Grants permission to describe a fraudster registration job	Read	domain* (p. 402)		
DescribeSpeaker	Grants permission to describe a speaker	Read	domain* (p. 402)		
DescribeSpeakerEnrollmentJob	Grants permission to describe a speaker enrollment job	Read	domain* (p. 402)		
EvaluateSession	Grants permission to evaluate a session	Write	domain* (p. 402)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDomains	Grants permission to list domains for an account	List			
ListFraudsterRegistrationJobs	Grants permission to list fraudster registration jobs for a domain	List	domain* (p. 402)		
ListSpeakerEnrollmentJobs	Grants permission to list speaker enrollment jobs for a domain	List	domain* (p. 402)		
ListSpeakers	Grants permission to list speakers for a domain	List	domain* (p. 402)		
ListTagsForResource	Grants permission to list tags for a Voice ID resource	Read	domain (p. 402)		
OptOutSpeaker	Grants permission to opt out a speaker	Write	domain* (p. 402)		
RegisterComplianceConsent	Grants permission to register compliance consent [permission only]	Write			
StartFraudsterRegistrationJob	Grants permission to start a fraudster registration job	Write	domain* (p. 402)		
StartSpeakerEnrollmentJob	Grants permission to start a speaker enrollment job	Write	domain* (p. 402)		
TagResource	Grants permission to tag a Voice ID resource	Tagging	domain (p. 402)		
				aws:RequestTag/\${TagKey} (p. 402)	
				aws:TagKeys (p. 402)	
UntagResource	Grants permission to remove a tag from a Voice ID resource	Tagging	domain (p. 402)		
				aws:TagKeys (p. 402)	
UpdateDomain	Grants permission to update a domain	Write	domain* (p. 402)		

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](#) (p. 400) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 402)

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 [Available global condition 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	String

Actions, resources, and condition keys for Amazon Connect Wisdom

Amazon Connect Wisdom (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 Connect Wisdom \(p. 402\)](#)
- [Resource types defined by Amazon Connect Wisdom \(p. 405\)](#)
- [Condition keys for Amazon Connect Wisdom \(p. 406\)](#)

Actions defined by Amazon Connect Wisdom

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

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

policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAssistant	Grants permission to create an assistant	Write		aws:TagKeys (p. 406) aws:RequestTag/\${TagKey} (p. 406)	
CreateAssistantAssociation	Grants permission to create an association between an assistant and another resource	Write	Assistant* (p. 405)		
				aws:TagKeys (p. 406) aws:RequestTag/\${TagKey} (p. 406)	
CreateContent	Grants permission to create content	Write	KnowledgeBase* (p. 406)		
				aws:TagKeys (p. 406) aws:RequestTag/\${TagKey} (p. 406)	
CreateKnowledgeBase	Grants permission to create a knowledge base	Write		aws:TagKeys (p. 406) aws:RequestTag/\${TagKey} (p. 406)	
CreateSession	Grants permission to create a session	Write	Assistant* (p. 405)		
				aws:TagKeys (p. 406) aws:RequestTag/\${TagKey} (p. 406)	
DeleteAssistant	Grants permission to delete an assistant	Write	Assistant* (p. 405)		
DeleteAssistantAssociation	Grants permission to delete an association	Write	Assistant* (p. 405)		
				AssistantAssociation* (p. 405)	
DeleteContent	Grants permission to delete content	Write	Content* (p. 406)		
				KnowledgeBase* (p. 406)	
DeleteKnowledgeBase	Grants permission to delete a knowledge base	Write	KnowledgeBase* (p. 406)		
GetAssistant	Grants permission to retrieve information about an assistant	Read	Assistant* (p. 405)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAssistantAssociation	Grants permission to retrieve information about an assistant association	Read	Assistant* (p. 405)		
			AssistantAssociation* (p. 405)		
GetContent	Grants permission to retrieve content, including a pre-signed URL to download the content	Read	Content* (p. 406)		
			KnowledgeBase* (p. 406)		
GetContentSummary	Grants permission to retrieve summary information about the content	Read	Content* (p. 406)		
			KnowledgeBase* (p. 406)		
GetKnowledgeBase	Grants permission to retrieve information about the knowledge base	Read	KnowledgeBase* (p. 406)		
GetRecommendation	Grants permission to retrieve recommendations for the specified session	Read	Assistant* (p. 405)		
GetSession	Grants permission to retrieve information for a specified session	Read	Assistant* (p. 405)		
			Session* (p. 406)		
ListAssistantAssociations	Grants permission to list information about assistant associations	List	Assistant* (p. 405)		
ListAssistants	Grants permission to list information about assistants	List			
ListContents	Grants permission to list the content with a knowledge base	List	KnowledgeBase* (p. 406)		
ListKnowledgeBases	Grants permission to list information about knowledge bases	List			
ListTagsForResource	Grants permission to list the tags for the specified resource	Read			
NotifyRecommendations	Grants permission to remove the specified recommendations from the specified assistant's queue of newly available recommendations	Write	Assistant* (p. 405)		
QueryAssistant	Grants permission to perform a manual search against the specified assistant	Read	Assistant* (p. 405)		
RemoveKnowledgeBase	Grants permission to remove a knowledge base	Write	KnowledgeBase* (p. 406)		

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* (p. 406)		
SearchSessions	Grants permission to search for sessions referencing a specified assistant. Can be used to get a specific session resource by its name	Read	Assistant* (p. 405)		
StartContentUpload	Grants permission to get a URL to upload content to a knowledge base	Write	KnowledgeBase* (p. 406)		
TagResource	Grants permission to add the specified tags to the specified resource	Tagging		aws:TagKeys (p. 406) aws:RequestTag/\${TagKey} (p. 406)	
UntagResource	Grants permission to remove the specified tags from the specified resource	Tagging		aws:TagKeys (p. 406)	
UpdateContent	Grants permission to update information about the content	Write	Content* (p. 406)		
UpdateKnowledgeBase	Grants permission to update the template URL of a knowledge base		KnowledgeBase* (p. 406)		

Resource types defined by Amazon Connect Wisdom

The following resource types are defined by this service and can be used in the Resource element of IAM permission policy statements. Each action in the [Actions table](#) (p. 402) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
Assistant	arn:\${Partition}:wisdom:\${Region}: \${Account}:assistant/\${AssistantId}	aws:ResourceTag/\${TagKey} (p. 406)
AssistantAssociation	arn:\${Partition}:wisdom:\${Region}: \${Account}:association/\${AssistantId}/\${AssistantAssociationId}	aws:ResourceTag/\${TagKey} (p. 406)

Resource types	ARN	Condition keys
Content	arn:\${Partition}:wisdom:\${Region}: \${Account}:content/\${KnowledgeBaseId}/ \${ContentId}	aws:ResourceTag/ \${TagKey} (p. 406)
KnowledgeBase	arn:\${Partition}:wisdom:\${Region}: \${Account}:knowledge-base/\${KnowledgeBaseId}	aws:ResourceTag/ \${TagKey} (p. 406)
Session	arn:\${Partition}:wisdom:\${Region}: \${Account}:session/\${AssistantId}/ \${SessionId}	aws:ResourceTag/ \${TagKey} (p. 406)

Condition keys for Amazon Connect Wisdom

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

To view the global condition keys that are available to all services, see [Available global condition 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	String

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 \(p. 407\)](#)
- [Resource types defined by AWS Connector Service \(p. 407\)](#)
- [Condition keys for AWS Connector Service \(p. 407\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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			
ValidateConnector [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

AWS 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 [Available keys for conditions](#).

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 \(p. 408\)](#)
- [Resource types defined by AWS Control Tower \(p. 411\)](#)
- [Condition keys for AWS Control Tower \(p. 411\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateManagedAccount [permission only]	Grants permission to create an account managed by AWS Control Tower.	Write			
DeregisterManagerAccount [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			
DescribeAccountFactory [permission only]	Grants permission to describe the current account factory configuration.	Read			
DescribeCoreServices [permission only]	Grants permission to describe resources managed by core accounts in AWS Control Tower.	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeGuardrail [permission only]	Grants permission to describe a guardrail.	Read			
DescribeGuardrail [permission only]	Grants permission to describe a guardrail for a organizational unit.	Read			
DescribeManagedAccount [permission only]	Grants permission to describe an account created through account factory.	Read			
DescribeManagedAWSOrganization [permission only]	Grants permission to describe an AWS Organization's organizational unit managed by AWS Control Tower.	Read			
DescribeSingleSignOn [permission only]	Grants permission to describe the current AWS Control Tower SSO configuration.	Read			
DisableGuardrail [permission only]	Grants permission to disable a guardrail from an organizational unit.	Write			
EnableGuardrail [permission only]	Grants permission to enable a guardrail to an organizational unit.	Write			
GetAvailableUpdates [permission only]	Grants permission to list available updates for the current AWS Control Tower deployment.	Read			
GetGuardrailComplianceStamp [permission only]	Grants permission to get the compliance status of a guardrail.	Read			
GetHomeRegion [permission only]	Grants permission to get the home region of the AWS Control Tower setup.	Read			
GetLandingZoneSetup [permission only]	Grants permission to get the current status of the landing zone setup.	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDirectoryGroups [permission only]	Grants permission to list the current directory groups available through SSO.	List			
ListEnabledGuardrails [permission only]	Grants permission to list currently enabled guardrails.	List			
ListGuardrailViolations [permission only]	Grants permission to list existing guardrail violations.	List			
ListGuardrails [permission only]	Grants permission to list all available guardrails.	List			
ListGuardrailsForOrganizationalUnit [permission only]	Grants permission to list Guardrails and their current state for a organizational unit.	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			
ListManagedAccountsForOrganizationalUnit [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			
ManageOrganizationUnit [permission only]	Grants permission to set up an organizational unit to be managed by AWS Control Tower.	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SetupLandingZone [permission only]	Grants permission to set up or update AWS Control Tower landing zone.	Write			
UpdateAccountFactoryConfiguration [permission only]	Grants permission to update the account factory configuration.	Write			

Resource types defined by AWS Control Tower

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

Condition keys for AWS Control Tower

AWS Control Tower 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 [Available keys for conditions](#).

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 \(p. 411\)](#)
- [Resource types defined by AWS Cost and Usage Report \(p. 412\)](#)
- [Condition keys for AWS Cost and Usage Report \(p. 412\)](#)

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

policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteReportDefinition	Delete Cost and Usage Report Definition	Write	cur* (p. 412)		
DescribeReportDefinition	Get Cost and Usage Report Definition	Read			
ModifyReportDefinition	Modify Cost and Usage Report Definition	Write	cur* (p. 412)		
PutReportDefinition	Write Cost and Usage Report Definition	Write	cur* (p. 412)		

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 \(p. 411\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
cur	<code>arn:\${Partition}:cur:\${Region}:\${Account}:definition/\${ReportName}</code>	

Condition keys for AWS Cost and Usage Report

Cost and Usage Report 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 [Available keys for conditions](#).

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 \(p. 413\)](#)
- [Resource types defined by AWS Cost Explorer Service \(p. 417\)](#)
- [Condition keys for AWS Cost Explorer Service \(p. 417\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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} (p. 417) aws:TagKeys (p. 418)	
CreateAnomalySubscription	Grants permission to create a new Anomaly Subscription	Write		aws:RequestTag/\${TagKey} (p. 417) aws:TagKeys (p. 418)	
CreateCostCategory	Grants permission to create a new Cost Category with the requested name and rules	Write		aws:RequestTag/\${TagKey} (p. 417) aws:TagKeys (p. 418)	
CreateNotificationReservation [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* (p. 417)		

Service Authorization Reference
Service Authorization Reference
AWS Cost Explorer Service

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/\${TagKey} (p. 418)	
DeleteAnomalySubscription	Grants permission to delete an Anomaly Subscription	Write	anomalysubscription* (p. 417)		
				aws:ResourceTag/\${TagKey} (p. 418)	
DeleteCostCategory	Grants permission to delete a Cost Category	Write	costcategory* (p. 417)		
				aws:ResourceTag/\${TagKey} (p. 418)	
DeleteNotificationReservation [permission only]	Grants permission to delete Reservation expiration alerts	Write			
DeleteReport [permission only]	Grants permission to delete Cost Explorer Reports	Write			
DescribeCostCategory	Grants permission to retrieve description such as the name, ARN, rules, definition, and effective dates of a Cost Category	Read	costcategory* (p. 417)		
				aws:ResourceTag/\${TagKey} (p. 418)	
DescribeNotificationReservation [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* (p. 417)		
				aws:ResourceTag/\${TagKey} (p. 418)	
GetAnomalyMonitor	Grants permission to query Anomaly Monitors	Read	anomalymonitor* (p. 417)		
				aws:ResourceTag/\${TagKey} (p. 418)	
GetAnomalySubscription	Grants permission to query Anomaly Subscriptions	Read	anomalysubscription* (p. 417)		
				aws:ResourceTag/\${TagKey} (p. 418)	
GetCostAndUsage	Grants permission to retrieve the cost and usage metrics for your account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCostAndUsage	Grants permission to retrieve the Cost and usage metrics with resources for your account	Read			
GetCostCategories	Grants permission to query Cost Category names and values for a specified time period	Read			
GetCostForecast	Grants permission to retrieve a cost forecast for a forecast time period	Read			
GetDimensionValues	Grants permission to retrieve all available filter values for a filter for a period of time	Read			
GetPreferences [permission only]	Grants permission to view Cost Explorer Preferences page	Read			
GetReservationCoverage	Grants permission to retrieve the reservation coverage for your account	Read			
GetReservationPurchaseRecommendations	Grants permission to retrieve the reservation purchase recommendations for your account	Read			
GetReservationUtilization	Grants permission to retrieve the reservation utilization for your account	Read			
GetRightsizingRecommendations	Grants permission to retrieve the rightsizing recommendations for your account	Read			
GetSavingsPlansCoverage	Grants permission to retrieve the Savings Plans coverage for your account	Read			
GetSavingsPlansRecommendations	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			

Service Authorization Reference
Service Authorization Reference
AWS Cost Explorer Service

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetUsageForecast	Grants permission to retrieve a usage forecast for a forecast time period	Read			
ListCostCategoryDefinitions	Grants permission to retrieve names, ARN, and effective dates for all Cost Categories	List			
ListTagsForResource	Grants permission to list tags for a Cost Explorer resource	Read	anomalymonitor (p. 417) anomalysubscription (p. 417)	costcategory (p. 417)	
			aws:ResourceTag/\${TagKey} (p. 418)		
ProvideAnomalyFeedback	Grants permission to provide Feedback on detected anomalies	Write			
TagResource	Grants permission to tag a Cost Explorer resource	Tagging	anomalymonitor (p. 417) anomalysubscription (p. 417)	costcategory (p. 417)	
	aws:TagKeys (p. 418)				
	aws:RequestTag/\${TagKey} (p. 417)				
	aws:ResourceTag/\${TagKey} (p. 418)				
UntagResource	Grants permission to remove tags from a Cost Explorer resource	Tagging	anomalymonitor (p. 417) anomalysubscription (p. 417)	costcategory (p. 417)	
	aws:TagKeys (p. 418)				
	aws:ResourceTag/\${TagKey} (p. 418)				
UpdateAnomalyMonitor	Grants permission to update an Existing Anomaly Monitor	Write	anomalymonitor* (p. 417)		
	aws:ResourceTag/\${TagKey} (p. 418)				
UpdateAnomalySubscription	Grants permission to update an Existing Anomaly Subscription	Write	anomalysubscription* (p. 417)		
	aws:ResourceTag/\${TagKey} (p. 418)				
UpdateCostCategory	Grants permission to update an Existing Cost Category	Write	costcategory* (p. 417)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/ \${TagKey} (p. 418)	
UpdateNotification [permission only]	Grants permission to update Reservation expiration alerts	Write			
UpdatePreference [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 \(p. 413\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 418)
anomalymonitor	arn:\${Partition}:ce::\${Account}:anomalymonitor/\${Identifier}	aws:ResourceTag/ \${TagKey} (p. 418)
costcategory	arn:\${Partition}:ce::\${Account}:costcategory/\${Identifier}	aws:ResourceTag/ \${TagKey} (p. 418)

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 [Available global condition keys](#).

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

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

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 \(p. 418\)](#)
- [Resource types defined by AWS Data Exchange \(p. 421\)](#)
- [Condition keys for AWS Data Exchange \(p. 421\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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	Write	jobs* (p. 421)		
CreateAsset [permission only]	Grants permission to create an asset (for example, in a Job)	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDataSet	Grants permission to create a data set	Write		aws:RequestTag/\${TagKey} (p. 421) aws:ResourceTag/\${TagKey} (p. 421) aws:TagKeys (p. 421)	
CreateEventAction	Grants permission to create an event action	Write	event-actions* (p. 421)		
CreateJob	Grants permission to create a job to import or export assets	Write	jobs* (p. 421)		
CreateRevision	Grants permission to create a revision	Write		aws:RequestTag/\${TagKey} (p. 421) aws:ResourceTag/\${TagKey} (p. 421) aws:TagKeys (p. 421)	
DeleteAsset	Grants permission to delete an asset	Write	assets* (p. 421)		
DeleteDataSet	Grants permission to delete a data set	Write	data-sets* (p. 421)		
DeleteEventAction	Grants permission to delete an event action	Write	event-actions* (p. 421)		
DeleteRevision	Grants permission to delete a revision	Write	revisions* (p. 421)		
GetAsset	Grants permission to get information about an asset and to export it (for example, in a Job)	Read	assets* (p. 421)		
GetDataSet	Grants permission to get information about a data set	Read	data-sets* (p. 421)		
GetEventAction	Grants permission to get an event action	Read	event-actions* (p. 421)		
GetJob	Grants permission to get information about a job	Read	jobs* (p. 421)		
GetRevision	Grants permission to get information about a revision	Read	revisions* (p. 421)		
ListDataSetRevisions	Grants permission to list the revisions of a data set	Read	revisions* (p. 421)		
ListDataSets	Grants permission to list data sets for the account	Read	data-sets* (p. 421)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListEventActions	Grants permission to list event actions for the account	Read	event-actions* (p. 421)		
ListJobs	Grants permission to list jobs for the account	Read	jobs* (p. 421)		
ListRevisionAssets	Grants permission to get list the assets of a revision	Read	assets* (p. 421)		
ListTagsForResource	Grants permission to list the tags that you associated with the specified resource	Read	data-sets (p. 421) revisions (p. 421)		
PublishDataSet [permission only]	Grants permission to publish a data set	Write	data-sets* (p. 421)		
RevokeRevision	Grants permission to revoke subscriber access to a revision	Write	revisions* (p. 421)		
SendApiAsset	Grants permission to send a request to an API asset	Write	assets* (p. 421)		
StartJob	Grants permission to start a job	Write	jobs* (p. 421)		
TagResource	Grants permission to add one or more tags to a specified resource	Tagging	data-sets (p. 421) revisions (p. 421) aws:RequestTag/\${TagKey} (p. 421) aws:TagKeys (p. 421)		
UntagResource	Grants permission to remove one or more tags from a specified resource	Tagging	data-sets (p. 421) revisions (p. 421) aws:TagKeys (p. 421)		
UpdateAsset	Grants permission to get update information about an asset	Write	assets* (p. 421)		
UpdateDataSet	Grants permission to update information about a data set	Write	data-sets* (p. 421)		
UpdateEventAction	Grants permission to update information for an event action	Write	event-actions* (p. 421)		
UpdateRevision	Grants permission to update information about a revision	Write	revisions* (p. 421)		

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 \(p. 418\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
jobs	<code>arn:\${Partition}:dataexchange:\${Region}: \${Account}:jobs/\${JobId}</code>	dataexchange:JobType (p. 421)
data-sets	<code>arn:\${Partition}:dataexchange:\${Region}: \${Account}:data-sets/\${DataSetId}</code>	aws:ResourceTag/ \${TagKey} (p. 421)
revisions	<code>arn:\${Partition}:dataexchange:\${Region}: \${Account}:data-sets/\${DataSetId}/revisions/ \${RevisionId}</code>	aws:ResourceTag/ \${TagKey} (p. 421)
assets	<code>arn:\${Partition}:dataexchange:\${Region}: \${Account}:data-sets/\${DataSetId}/revisions/ \${RevisionId}/assets/\${AssetId}</code>	
event-actions	<code>arn:\${Partition}:dataexchange:\${Region}: \${Account}:event-actions/\${EventActionId}</code>	

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 [Available global condition 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 \(p. 422\)](#)
- [Resource types defined by Amazon Data Lifecycle Manager \(p. 423\)](#)
- [Condition keys for Amazon Data Lifecycle Manager \(p. 423\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("`*`") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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} (p. 424) aws:TagKeys (p. 424)	
DeleteLifecyclePolicy	Grants permission to delete an existing data lifecycle policy. In addition, this action halts the creation and deletion of snapshots that the policy	Write	policy* (p. 423)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	specified. Existing snapshots are not affected				
GetLifecyclePolicies	Grants permission to returns a list of summary descriptions of data lifecycle policies	List			
GetLifecyclePolicy	Grants permission to return a complete description of a single data lifecycle policy	Read	policy* (p. 423)		
ListTagsForResource	Grants permission to list the tags associated with a resource	Read	policy* (p. 423)		
TagResource	Grants permission to add or update tags of a resource	Tagging	policy* (p. 423)		
				aws:RequestTag/\${TagKey} (p. 424) aws:TagKeys (p. 424)	
UntagResource	Grants permission to remove tags associated with a resource	Tagging	policy* (p. 423)		
				aws:RequestTag/\${TagKey} (p. 424) aws:TagKeys (p. 424)	
UpdateLifecyclePolicy	Grants permission to update an existing data lifecycle policy	Write	policy* (p. 423)		

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](#) (p. 422) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
policy	<code>arn:\${Partition}:dlm:\${Region}:\${Account}:policy/\${ResourceName}</code>	aws:ResourceTag/\${TagKey} (p. 424)

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 [Available global condition 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 \(p. 424\)](#)
- [Resource types defined by AWS Data Pipeline \(p. 427\)](#)
- [Condition keys for AWS Data Pipeline \(p. 427\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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	Write			datapipeline:PipelineCreator (p. 427) datapipeline:Tag (p. 427)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	the pipeline does not pass validation, activation fails				datipeline:workerGroup (p. 427)
AddTags	Grants permission to add or modify tags for the specified pipeline	Tagging			datipline:PipelineCreator (p. 427) datipline:Tag (p. 427)
CreatePipeline	Grants permission to create a new, empty pipeline	Write			aws:RequestTag/\${TagKey} (p. 427) aws:TagKeys (p. 427) datipline:Tag (p. 427)
DeactivatePipeline	Grants permission to Deactivate the specified running pipeline	Write			datipline:PipelineCreator (p. 427) datipline:Tag (p. 427) datipline:workerGroup (p. 427)
DeletePipeline	Grants permission to delete a pipeline, its pipeline definition, and its run history	Write			datipline:PipelineCreator (p. 427) datipline:Tag (p. 427)
DescribeObjects	Grants permission to get the object definitions for a set of objects associated with the pipeline	Read			datipline:PipelineCreator (p. 427) datipline:Tag (p. 427)
DescribePipelines	Grants permission to retrieves metadata about one or more pipelines	List			datipline:PipelineCreator (p. 427) datipline:Tag (p. 427)
EvaluateExpression	Grants permission to task runners to call EvaluateExpression, to evaluate a string in the context of the specified object	Read			datipline:PipelineCreator (p. 427) datipline:Tag (p. 427)
GetAccountLimits	Grants permission to call GetAccountLimits	List			
GetPipelineDefinition	Grants permission to gets the definition of the specified pipeline	Read			datipline:PipelineCreator (p. 427) datipline:Tag (p. 427) datipline:workerGroup (p. 427)
ListPipelines	Grants permission to list the pipeline identifiers for all active pipelines that you have permission to access	List			

Service Authorization Reference
Service Authorization Reference
AWS Data Pipeline

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PollForTask	Grants permission to task runners to call PollForTask, to receive a task to perform from AWS Data Pipeline	Write			datipeline:workerGroup (p. 427)
PutAccountLimits	Grants permission to call PutAccountLimits	Write			
PutPipelineDefinition	Grants permission to add tasks, schedules, and preconditions to the specified pipeline	Write		datipline:PipelineCreator (p. 427)	datipline:Tag (p. 427)
QueryObjects	Grants permission to query the specified pipeline for the names of objects that match the specified set of conditions	Read		datipline:PipelineCreator (p. 427)	datipline:Tag (p. 427)
RemoveTags	Grants permission to remove existing tags from the specified pipeline	Tagging		datipline:PipelineCreator (p. 427)	datipline:Tag (p. 427)
ReportTaskProgress	Grants permission to task runners to call ReportTaskProgress, when they are assigned a task to acknowledge that it has the task	Write			
ReportTaskRunnerHeartbeat	Grants permission to task runners to call ReportTaskRunnerHeartbeat every 15 minutes to indicate that they are operational	Write			
SetStatus	Grants permission to requests that the status of the specified physical or logical pipeline objects be updated in the specified pipeline	Write		datipline:PipelineCreator (p. 427)	datipline:Tag (p. 427)
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			
ValidatePipelineDefinition	Grants permission to validate the specified pipeline definition to ensure that it is well formed and can be run without error	Read		datipline:PipelineCreator (p. 427)	datipline:Tag (p. 427)
					datipline:workerGroup (p. 427)

Resource types defined by AWS Data Pipeline

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

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters access by the presence of tag key-value pairs in the request	String
<code>aws:TagKeys</code>	Filters access by the presence of tag keys in the request	ArrayOfString
<code>datapipeline:PipelineCreator</code>	Filters access by the IAM user that created the pipeline	ArrayOfString
<code>datapipeline:Tag</code>	Filters access by customer-specified key/value pair that can be attached to a resource	ArrayOfString
<code>datapipeline:workerGroupTaskRunner</code>	Filters access by the name of a worker group for which a TaskRunner 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 \(p. 427\)](#)
- [Resource types defined by AWS Database Migration Service \(p. 433\)](#)
- [Condition keys for AWS Database Migration Service \(p. 434\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 (p. 433) Endpoint (p. 433) EventSubscription (p. 434) ReplicationInstance (p. 434) ReplicationSubnetGroup (p. 434) ReplicationTask (p. 434)	aws:RequestTag/ {\$TagKey} (p. 434) aws:TagKeys (p. 434) dms:req- tag/ {\$TagKey} (p. 435)	
ApplyPendingMaintenance	Grants permission to apply a pending maintenance action to a resource (for example, to a replication instance)	Write		ReplicationInstance* (p. 434)	
CancelReplicationTaskAssessmentRun	Grants permission to cancel a single pending assessment run	Write		ReplicationTaskAssessmentRun* (p. 434)	
CreateEndpoint	Grants permission to create an endpoint using the provided settings	Write		aws:RequestTag/ {\$TagKey} (p. 434) aws:TagKeys (p. 434) dms:req- tag/ {\$TagKey} (p. 435)	
CreateEventSubscription	Grants permission to create an AWS DMS event notification subscription	Write		aws:RequestTag/ {\$TagKey} (p. 434) aws:TagKeys (p. 434)	AWS DMS

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				dms:req-tag/\${TagKey} (p. 435)	
CreateReplicationTask	Grants permission to create a replication instance using the specified parameters	Write		aws:RequestTag/\${TagKey} (p. 434) aws:TagKeys (p. 434) dms:req-tag/\${TagKey} (p. 435)	
CreateReplicationSubnetGroup	Grants permission to create a replication subnet group given a list of the subnet IDs in a VPC	Write		aws:RequestTag/\${TagKey} (p. 434) aws:TagKeys (p. 434) dms:req-tag/\${TagKey} (p. 435)	
CreateReplicationTask	Grants permission to create a replication task using the specified parameters	Write	Endpoint* (p. 433)		
			ReplicationInstance* (p. 434)		
			aws:RequestTag/\${TagKey} (p. 434) aws:TagKeys (p. 434) dms:req-tag/\${TagKey} (p. 435)		
DeleteCertificate	Grants permission to delete the specified certificate	Write	Certificate* (p. 433)		
DeleteConnection	Grants permission to delete the specified connection between a replication instance and an endpoint	Write	Endpoint* (p. 433)		
			ReplicationInstance* (p. 434)		
DeleteEndpoint	Grants permission to delete the specified endpoint	Write	Endpoint* (p. 433)		
DeleteEventSubscription	Grants permission to delete an AWS DMS event subscription	Write	EventSubscription* (p. 434)		
DeleteReplicationInstance	Grants permission to delete the specified replication instance	Write	ReplicationInstance* (p. 434)		
DeleteReplicationSubnetGroup	Grants permission to delete a subnet group	Write	ReplicationSubnetGroup* (p. 434)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteReplicationTask	Grants permission to delete the specified replication task	Write	ReplicationTask* (p. 434)		
DeleteReplicationTaskAssessmentRun	Grants permission to delete the records of a single premigration assessment run	Write	ReplicationTaskAssessmentRun* (p. 434)		
DescribeAccount	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 (p. 434)		
			ReplicationTask (p. 434)		
DescribeCertificate	Grants permission to provide a description of the certificate	Read			
DescribeConnection	Grants permission to describe the status of the connections that have been made between the replication instance and an endpoint	Read			
DescribeEndpoint	Grants permission to return the possible endpoint settings available when you create an endpoint for a specific database engine	Read			
DescribeEndpointType	Grants permission to return information about the type of endpoints available	Read			
DescribeEndpoint	Grants permission to return information about the endpoints for your account in the current region	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			
DescribeEvents	Grants permission to list events for a given source identifier and source type	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeOrderableReplicationInstanceTypes	Grants permission to return information about the replication instance types that can be created in the specified region	Read			
DescribeRefreshSchemasStatus	Grants permission to returns the status of the RefreshSchemas operation	Read	Endpoint* (p. 433)		
DescribeReplicationTaskLogs	Grants permission to return information about the task logs for the specified task	Read	ReplicationInstance* (p. 434)	aws:ResourceTag/\${TagKey} (p. 434)	aws:TagKeys (p. 434)
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			
DescribeReplicationTaskAssessmentRuns	Grants permission to return the latest task assessment results from Amazon S3	Read	ReplicationTask (p. 434)		
DescribeReplicationTaskAssessments	Grants permission to return a paginated list of migration assessment runs based on filter settings	Read	ReplicationInstance (p. 434)	ReplicationTask (p. 434)	ReplicationTaskAssessmentRun (p. 434)
DescribeReplicationTasks	Grants permission to return a paginated list of individual assessments based on filter settings	Read	ReplicationTask (p. 434)	ReplicationTaskAssessmentRun (p. 434)	
DescribeReplicationTasksForRegion	Grants permission to return information about replication tasks for your account in the current region	Read			
DescribeSchemas	Grants permission to return information about the schema for the specified endpoint	Read	Endpoint* (p. 433)		
DescribeTableStatistics	Grants permission to return table statistics on the database migration task, including table name, rows inserted, rows updated, and rows deleted	Read	ReplicationTask* (p. 434)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportCertificate	Grants permission to upload the specified certificate	Write		aws:RequestTag/ \${TagKey} (p. 434)	
ListTagsForResource	Grants permission to list all tags for an AWS DMS resource	Read	Certificate (p. 433)		
	Endpoint (p. 433)				
	EventSubscription (p. 434)				
	ReplicationInstance (p. 434)				
	ReplicationSubnetGroup (p. 434)				
	ReplicationTask (p. 434)				
ModifyEndpoint	Grants permission to modify the specified endpoint	Write	Endpoint* (p. 433)		
ModifyEventSubscription	Grants permission to modify an existing AWS DMS event notification subscription	Write			
ModifyReplicationInstance	Grants permission to modify the replication instance to apply new settings	Write	ReplicationInstance* (p. 434)		
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* (p. 434)		
MoveReplicationTask	Grants permission to move the specified replication task to a different replication instance	Write	ReplicationInstance* (p. 434)		
			ReplicationTask* (p. 434)		
RebootReplicationInstance	Grants permission to reboot a replication instance. Rebooting results in a momentary outage, until the replication instance becomes available again	Write	ReplicationInstance* (p. 434)		
RefreshSchemas	Grants permission to populate the schema for the specified endpoint	Write	Endpoint* (p. 433)		
			ReplicationInstance* (p. 434)		
ReloadTables	Grants permission to reload the target database table with the source data	Write	ReplicationTask* (p. 434)		
RemoveTagsFromResource	Grants permission to remove metadata tags from a DMS resource	Tagging	Certificate (p. 433)		
			Endpoint (p. 433)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			EventSubscription (p. 434) ReplicationInstance (p. 434) ReplicationSubnetGroup (p. 434) ReplicationTask (p. 434)		aws:TagKeys (p. 434)
StartReplicationTask	Grants permission to start the replication task	Write	ReplicationTask* (p. 434)		
StartReplicationTaskAssessment	Grants permission to start the replication task assessment for unsupported data types in the source database	Write	ReplicationTask* (p. 434)		
StartReplicationTaskMigrationAssessment	Grants permission to start a migration assessment run for one or more individual assessments of a migration task	Write	ReplicationTask* (p. 434)		
StopReplicationTask	Grants permission to stop the replication task	Write	ReplicationTask* (p. 434)		
TestConnection	Grants permission to test the connection between the replication instance and the endpoint	Read	Endpoint* (p. 433)		
			ReplicationInstance* (p. 434)		

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 \(p. 427\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 434) dms:cert-tag/\${TagKey} (p. 434)
Endpoint	arn:\${Partition}:dms:\${Region}:\${Account}:endpoint:*	aws:ResourceTag/\${TagKey} (p. 434) dms:endpoint-tag/\${TagKey} (p. 434)

Resource types	ARN	Condition keys
EventSubscription	arn:\${Partition}:dms:\${Region}:\${Account}:es:*	aws:ResourceTag/\${TagKey} (p. 434) dms:es-tag/\${TagKey} (p. 435)
ReplicationInstance	arn:\${Partition}:dms:\${Region}:\${Account}:rep:*	aws:ResourceTag/\${TagKey} (p. 434) dms:rep-tag/\${TagKey} (p. 435)
ReplicationSubnetGroup	arn:\${Partition}:dms:\${Region}:\${Account}:subgrp:*	aws:ResourceTag/\${TagKey} (p. 434) dms:subgrp-tag/\${TagKey} (p. 435)
ReplicationTask	arn:\${Partition}:dms:\${Region}:\${Account}:task:*	aws:ResourceTag/\${TagKey} (p. 434) dms:task-tag/\${TagKey} (p. 435)
ReplicationTaskAssessmentRun	arn:\${Partition}:dms:\${Region}:\${Account}:assessment-run:*	
ReplicationTaskIndividualAssessment	arn:\${Partition}:dms:\${Region}:\${Account}:individual-assessment:*	

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 [Available global condition keys](#).

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

Condition keys	Description	Type
dms:es-tag/ \${TagKey}	Filters access based on the presence of tag keys in the request for EventSubscription	String
dms:rep-tag/ \${TagKey}	Filters access based on the presence of tag keys in the request for ReplicationInstance	String
dms:req-tag/ \${TagKey}	Filters access based on the presence of tag key-value pairs in the request	String
dms:subgrp-tag/ \${TagKey}	Filters access based on the presence of tag keys in the request for ReplicationSubnetGroup	String
dms:task-tag/ \${TagKey}	Filters access based on the presence of tag keys 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 \(p. 435\)](#)
- [Resource types defined by Database Query Metadata Service \(p. 436\)](#)
- [Condition keys for Database Query Metadata Service \(p. 436\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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			
DeleteFavoriteQuery	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			
DescribeQueryHistories	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			
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 [Available keys for conditions](#).

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 \(p. 437\)](#)
- [Resource types defined by AWS DataSync \(p. 441\)](#)
- [Condition keys for AWS DataSync \(p. 441\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelTaskExecution	Grants permission to cancel execution of a sync task	Write	taskexecution* (p. 441)		
CreateAgent	Grants permission to activate an agent that you have deployed on your host	Write		aws:RequestTag/\${TagKey} (p. 441) aws:TagKeys (p. 441)	
CreateLocationEndpoint	Grants permission to create an endpoint for an Amazon EFS file system	Write		aws:RequestTag/\${TagKey} (p. 441) aws:TagKeys (p. 441)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLocationFsxLustreEndpoint	Grants permission to create an endpoint for an Amazon FSx Lustre	Write		aws:RequestTag/ \${TagKey} (p. 441) aws:TagKeys (p. 441)	
CreateLocationFsxOpenZFSEndpoint	Grants permission to create an endpoint for Amazon FSx for OpenZFS	Write		aws:RequestTag/ \${TagKey} (p. 441) aws:TagKeys (p. 441)	
CreateLocationFsxWindowsEndpoint	Grants permission to create an endpoint for an Amazon FSx Windows File Server file system	Write		aws:RequestTag/ \${TagKey} (p. 441) aws:TagKeys (p. 441)	
CreateLocationHdfsEndpoint	Grants permission to create an endpoint for an Amazon Hdfs	Write		aws:RequestTag/ \${TagKey} (p. 441) aws:TagKeys (p. 441)	
CreateLocationNfsEndpoint	Grants permission to create an endpoint for a NFS file system	Write		aws:RequestTag/ \${TagKey} (p. 441) aws:TagKeys (p. 441)	
CreateLocationObjectStorageEndpoint	Grants permission to create an endpoint for a self-managed object storage bucket	Write		aws:RequestTag/ \${TagKey} (p. 441) aws:TagKeys (p. 441)	
CreateLocationS3Endpoint	Grants permission to create an endpoint for an Amazon S3 bucket	Write		aws:RequestTag/ \${TagKey} (p. 441) aws:TagKeys (p. 441)	
CreateLocationSmbEndpoint	Grants permission to create an endpoint for an SMB file system	Write		aws:RequestTag/ \${TagKey} (p. 441) aws:TagKeys (p. 441)	
CreateTask	Grants permission to create a sync task	Write		aws:RequestTag/ \${TagKey} (p. 441) aws:TagKeys (p. 441)	
DeleteAgent	Grants permission to delete an agent	Write	agent* (p. 441)		
DeleteLocation	Grants permission to delete a location used by AWS DataSync	Write	location* (p. 441)		
DeleteTask	Grants permission to delete a sync task	Write	task* (p. 441)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeAgent	Grants permission to view metadata such as name, network interfaces, and the status (that is, whether the agent is running or not) about a sync agent	Read	agent* (p. 441)		
DescribeLocationEFS	Grants permission to view metadata, such as the path information about an Amazon EFS sync location	Read	location* (p. 441)		
DescribeLocationFSxLustre	Grants permission to view metadata, such as the path information about an Amazon FSx Lustre sync location	Read	location* (p. 441)		
DescribeLocationFSxOpenZFS	Grants permission to view metadata, such as the path information about an Amazon FSx OpenZFS sync location	Read	location* (p. 441)		
DescribeLocationFSxWindows	Grants permission to view metadata, such as the path information about an Amazon FSx Windows sync location	Read	location* (p. 441)		
DescribeLocationHDFS	Grants permission to view metadata, such as the path information about an Amazon HDFS sync location	Read	location* (p. 441)		
DescribeLocationNFS	Grants permission to view metadata, such as the path information, about a NFS sync location	Read	location* (p. 441)		
DescribeLocationObjectStorage	Grants permission to view metadata about a self-managed object storage server location	Read	location* (p. 441)		
DescribeLocationS3	Grants permission to view metadata, such as bucket name, about an Amazon S3 bucket sync location	Read	location* (p. 441)		
DescribeLocationSmb	Grants permission to view metadata, such as the path information, about an SMB sync location	Read	location* (p. 441)		
DescribeTask	Grants permission to view metadata about a sync task	Read	task* (p. 441)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeTaskExecutionMetadata	Grants permission to view metadata about a sync task that is being executed	Read	taskexecution* (p. 441)		
ListAgents	Grants permission to list agents owned by an AWS account in a region specified in the request	List			
ListLocations	Grants permission to list source and destination sync locations	List			
ListTagsForResource	Grants permission to list tags that have been added to the specified resource	Read	agent (p. 441) location (p. 441) task (p. 441)		
ListTaskExecutionMetadata	Grants permission to list executed sync tasks	List			
ListTasks	Grants permission to list of all the sync tasks	List			
StartTaskExecution	Grants permission to start a specific invocation of a sync task	Write	task* (p. 441)		
TagResource	Grants permission to apply a key-value pair to an AWS resource	Tagging	agent (p. 441) location (p. 441) task (p. 441) aws:RequestTag/\${TagKey} (p. 441) aws:TagKeys (p. 441)		
UntagResource	Grants permission to remove one or more tags from the specified resource	Tagging	agent (p. 441) location (p. 441) task (p. 441) aws:TagKeys (p. 441)		
UpdateAgent	Grants permission to update the name of an agent	Write	agent* (p. 441)		
UpdateLocationHDFS	Grants permission to update an HDFS sync Location	Write	location* (p. 441)		
UpdateLocationNFS	Grants permission to update an NFS sync Location	Write	location* (p. 441)		
UpdateLocationObjectStorage	Grants permission to update a self-managed object storage server location	Write	location* (p. 441)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateLocationSMB	Grants permission to update a SMB sync location	Write	location* (p. 441)		
UpdateTask	Grants permission to update metadata associated with a sync task	Write	task* (p. 441)		
UpdateTaskExecution	Grants permission to update execution of a sync task	Write	taskexecution* (p. 441)		

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 \(p. 437\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
agent	<code>arn:\${Partition}:datasync:\${Region}: \${AccountId}:agent/\${AgentId}</code>	aws:ResourceTag/\${TagKey} (p. 441)
location	<code>arn:\${Partition}:datasync:\${Region}: \${AccountId}:location/\${LocationId}</code>	aws:ResourceTag/\${TagKey} (p. 441)
task	<code>arn:\${Partition}:datasync:\${Region}: \${AccountId}:task/\${TaskId}</code>	aws:ResourceTag/\${TagKey} (p. 441)
taskexecution	<code>arn:\${Partition}:datasync:\${Region}: \${AccountId}:task/\${TaskId}/execution/\${ExecutionId}</code>	

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 [Available global condition keys](#).

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

Actions, resources, and condition keys for AWS DeepComposer

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

References:

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

Topics

- [Actions defined by AWS DeepComposer \(p. 442\)](#)
- [Resource types defined by AWS DeepComposer \(p. 444\)](#)
- [Condition keys for AWS DeepComposer \(p. 445\)](#)

Actions defined by AWS DeepComposer

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

The **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateCoupon [permission only]	Grants permission to associate a DeepComposer coupon (or DSN) with the account associated with the sender of the request	Write			
CreateAudio [permission only]	Grants permission to create an audio file by converting the midi composition into a wav or mp3 file	Write	audio* (p. 445)		
CreateComposition [permission only]	Grants permission to create a multi-track midi composition	Write	composition* (p. 445)	aws:RequestTag/\${TagKey} (p. 445)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					aws:TagKeys (p. 445)
CreateModel [permission only]	Grants permission to start creating/training a generative-model that is able to perform inference against the user-provided piano-melody to create a multi-track midi composition	Write	model* (p. 444)		
				aws:RequestTag/ \${TagKey} (p. 445)	
				aws:TagKeys (p. 445)	
DeleteComposition [permission only]	Grants permission to delete the composition	Write	composition* (p. 445)		
DeleteModel	Grants permission to delete the model	Write		model* (p. 444)	
GetComposition [permission only]	Grants permission to get information about the composition	Read	composition* (p. 445)		
				aws:ResourceTag/ \${TagKey} (p. 445)	
GetModel [permission only]	Grants permission to get information about the model	Read	model* (p. 444)		
				aws:ResourceTag/ \${TagKey} (p. 445)	
GetSampleModel [permission only]	Grants permission to get information about the sample/pre-trained DeepComposer model	Read	model* (p. 444)		
ListCompositions [permission only]	Grants permission to list all the compositions owned by the sender of the request	List	composition* (p. 445)		
ListModels [permission only]	Grants permission to list all the models owned by the sender of the request	List	model* (p. 444)		
ListSampleModels [permission only]	Grants permission to list all the sample/pre-trained models provided by the DeepComposer service	List	model* (p. 444)		
ListTagsForResource	Grants permission to list tags for a resource	List	composition (p. 445) model (p. 444) aws:ResourceTag/ \${TagKey} (p. 445)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTrainingTopics [permission only]	Grants permission to list all the training options or topic for creating/training a model	List	model* (p. 444)		
TagResource	Grants permission to tag a resource	Tagging	composition (p. 445) model (p. 444)	aws:TagKeys (p. 445)	
				aws:RequestTag/ {\$TagKey} (p. 445)	
UntagResource	Grants permission to untag a resource	Tagging	composition (p. 445) model (p. 444)	aws:ResourceTag/ {\$TagKey} (p. 445)	
UpdateComposition [permission only]	Grants permission to modify the mutable properties associated with a composition	Write	composition* (p. 445)		
UpdateModel [permission only]	Grants permission to modify the mutable properties associated with a model	Write	model* (p. 444)		

Resource types defined by AWS DeepComposer

The following resource types are defined by this service and can be used in the Resource element of IAM permission policy statements. Each action in the [Actions table \(p. 442\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
model	arn:\${Partition}:deepcomposer:\${Region}: \${Account}:model/\${ModelId}	aws:ResourceTag/ {\$TagKey} (p. 445)

Resource types	ARN	Condition keys
composition	arn:\${Partition}:deepcomposer:\${Region}: \${Account}:composition/\${CompositionId}	aws:ResourceTag/\${TagKey} (p. 445)
audio	arn:\${Partition}:deepcomposer:\${Region}: \${Account}:audio/\${AudioId}	

Condition keys for AWS DeepComposer

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

To view the global condition keys that are available to all services, see [Available global condition 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 DeepLens

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

Topics

- [Actions defined by AWS DeepLens \(p. 445\)](#)
- [Resource types defined by AWS DeepLens \(p. 447\)](#)
- [Condition keys for AWS DeepLens \(p. 448\)](#)

Actions defined by AWS DeepLens

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

The **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateServiceRoleToAccount	Associates the user's account controlling various permissions needed by AWS DeepLens for proper functionality.	Permissions management			
BatchGetDevice	Retrieves a list of AWS DeepLens devices.	Read	device* (p. 447)		
BatchGetModel	Retrieves a list of AWS DeepLens Models.	Read	model* (p. 447)		
BatchGetProject	Retrieves a list of AWS DeepLens Projects.	Read	project* (p. 447)		
CreateDeviceCertificate	Creates a certificate package that is used to successfully authenticate and Register an AWS DeepLens device.	Write			
CreateModel	Creates a new AWS DeepLens Model.	Write			
CreateProject	Creates a new AWS DeepLens Project.	Write			
DeleteModel	Deletes an AWS DeepLens Model.	Write	model* (p. 447)		
DeleteProject	Deletes an AWS DeepLens Project.	Write	project* (p. 447)		
DeployProject	Deploys an AWS DeepLens project to a registered AWS DeepLens device.	Write	device* (p. 447) project* (p. 447)		
DeregisterDevice	Begins a device de-registration workflow for a registered AWS DeepLens device.	Write	device* (p. 447)		
GetAssociatedResources	Retrieves the account level resources associated with the user's account.	Read			
GetDeploymentStatus	Retrieves the deployment status of a particular AWS DeepLens device, along with any associated metadata.	Read			
GetDevice	Retrieves information about an AWS DeepLens device.	Read	device* (p. 447)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetModel	Retrieves an AWS DeepLens Model.	Read	model* (p. 447)		
GetProject	Retrieves an AWS DeepLens Project.	Read	project* (p. 447)		
ImportProjectFromTemplate	Creates a new AWS DeepLens Project from a sample project template.	Write			
ListDeployments	Retrieves a list of AWS DeepLens Deployment identifiers.	List			
ListDevices	Retrieves a list of AWS DeepLens device identifiers.	List			
ListModels	Retrieves a list of AWS DeepLens Model identifiers.	List			
ListProjects	Retrieves a list of AWS DeepLens Project identifiers.	List			
RegisterDevice	Begins a device registration workflow for an AWS DeepLens device.	Write			
RemoveProject	Removes a deployed AWS DeepLens project from an AWS DeepLens device.	Write	device* (p. 447)		
UpdateProject	Updates an existing AWS DeepLens Project.	Write	project* (p. 447)		

Resource types defined by AWS DeepLens

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the [Actions table \(p. 445\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
device	<code>arn:\${Partition}:deelens:\${Region}: \${Account}:device/\${DeviceName}</code>	
project	<code>arn:\${Partition}:deelens:\${Region}: \${Account}:project/\${ProjectName}</code>	
model	<code>arn:\${Partition}:deelens:\${Region}: \${Account}:model/\${ModelName}</code>	

Condition keys for AWS DeepLens

DeepLens 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 [Available keys for conditions](#).

Actions, resources, and condition keys for AWS DeepRacer

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

References:

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

Topics

- [Actions defined by AWS DeepRacer \(p. 448\)](#)
- [Resource types defined by AWS DeepRacer \(p. 455\)](#)
- [Condition keys for AWS DeepRacer \(p. 456\)](#)

Actions defined by AWS DeepRacer

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

The **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddLeaderboard AdminGetAccountConfig [permission only]	Grants permission to add access for a <code>PrivateLeaderboard</code> [permission only]	Write	leaderboard* (p. 455)		
				depracer:UserToken (p. 456) depracer:MultiUser (p. 456)	
	Grants permission to get current <code>AdminConfig</code> multiuser configuration for this account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
[permission only]					
AdminListAssociatedUsers [permission only]	Grants permission to list all DeepRacer users with their associated resources created under this account	Read			
AdminListAssociatedDataForUser [permission only]	Grants permission to list user data for all users associated with this account	Read			
AdminManageUser [permission only]	Grants permission to manage a user associated with this account	Write			
AdminSetAccountConfiguration [permission only]	Grants permission to set configuration options for this account	Write			
CloneReinforcementLearningModel [permission only]	Grants permission to clone an existing DeepRacer model	Write	reinforcement_learning_model* (p. 455)		
			track* (p. 455)		
CreateCar [permission only]	Grants permission to create a DeepRacer car in your garage	Write		aws:RequestTag/\${TagKey} (p. 456) aws:TagKeys (p. 456) deepracer:UserToken (p. 456) deepracer:MultiUser (p. 456)	
CreateLeaderboard [permission only]	Grants permission to create a DeepRacer leaderboard	Write		aws:RequestTag/\${TagKey} (p. 456) aws:TagKeys (p. 456) deepracer:UserToken (p. 456) deepracer:MultiUser (p. 456)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLeaderboard [permission only]	Grants permission to create a DeepRacer model to be evaluated for leaderboards	Write	leaderboard* (p. 455)	deepracer:UserToken (p. 456)	deepracer:MultiUser (p. 456)
CreateLeaderboard [permission only]	Grants permission to create a DeepRacer model to be evaluated for leaderboards	Write	leaderboard* (p. 455) reinforcement_learning_model* (p. 455)	aws:RequestTag/ \${TagKey} (p. 456) aws:TagKeys (p. 456)	deepracer:UserToken (p. 456) deepracer:MultiUser (p. 456)
CreateReinforcementLearningModel [permission only]	Grants permission to create a reinforcement learning model for DeepRacer	Write	track* (p. 455)	aws:RequestTag/ \${TagKey} (p. 456) aws:TagKeys (p. 456)	deepracer:UserToken (p. 456) deepracer:MultiUser (p. 456)
DeleteLeaderboard [permission only]	Grants permission to delete a DeepRacer model	Write	leaderboard* (p. 455)	deepracer:UserToken (p. 456)	deepracer:MultiUser (p. 456)
DeleteModel [permission only]	Grants permission to edit a DeepRacer model	Write	reinforcement_learning_model* (p. 455)	deepracer:UserToken (p. 456)	deepracer:MultiUser (p. 456)
EditLeaderboard [permission only]	Grants permission to edit a DeepRacer model	Write	leaderboard* (p. 455)	deepracer:UserToken (p. 456)	deepracer:MultiUser (p. 456)
GetAccountConfig [permission only]	Grants permission to get current multiuser configuration for this account	Read		deepracer:UserToken (p. 456)	deepracer:MultiUser (p. 456)
GetAlias [permission only]	Grants permission to retrieve the user's alias for submitting a DeepRacer model to leaderboards	Read		deepracer:UserToken (p. 456)	deepracer:MultiUser (p. 456)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAssetUrl [permission only]	Grants permission to download artifacts for an existing DeepRacer model	Read	reinforcement_learning_model* (p. 455)		
			depracer:UserToken (p. 456)		
GetCar [permission only]	Grants permission to retrieve a specific DeepRacer car from your garage	Read	car* (p. 455)		
			depracer:UserToken (p. 456)		
GetCars [permission only]	Grants permission to view all the DeepRacer cars in your garage	Read	depracer:MultiUser (p. 456)		
GetEvaluation [permission only]	Grants permission to retrieve information about an existing DeepRacer model's evaluation jobs	Read	evaluation_job* (p. 455)		
			depracer:UserToken (p. 456)		
GetLatestUserSubmission [permission only]	Grants permission to retrieve information about how the latest submitted DeepRacer model for a user performed on a leaderboard	Read	leaderboard* (p. 455)		
			depracer:UserToken (p. 456)		
GetLeaderboard [permission only]	Grants permission to retrieve information about leaderboards	Read	depracer:MultiUser (p. 456)		
GetModel [permission only]	Grants permission to retrieve information about an existing DeepRacer model	Read	reinforcement_learning_model* (p. 455)		
			depracer:UserToken (p. 456)		
GetPrivateLeaderboard [permission only]	Grants permission to retrieve information about private leaderboards	Read	depracer:MultiUser (p. 456)		
			depracer:UserToken (p. 456)		
GetRankedUserSubmission [permission only]	Grants permission to retrieve information about the performance of a user's DeepRacer model that got placed on a leaderboard	Read	depracer:UserToken (p. 456)		
			depracer:MultiUser (p. 456)		
			track* (p. 455)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTrainingJob [permission only]	Grants permission to retrieve information about an existing DeepRacer model's training job	Read	training_job* (p. 455)		
	deepracer:UserToken (p. 456)		deepracer:MultiUser (p. 456)		
ImportModel [permission only]	Grants permission to import a reinforcement learning model for DeepRacer	Write		deepracer:UserToken (p. 456)	deepracer:MultiUser (p. 456)
ListEvaluations [permission only]	Grants permission to list a DeepRacer model's evaluation jobs	Read	reinforcement_learning_model* (p. 455)		
	deepracer:UserToken (p. 456)		deepracer:MultiUser (p. 456)		
ListLeaderboardSubmissions [permission only]	Grants permission to list all the DeepRacer model submissions of a user on a leaderboard	Read	leaderboard* (p. 455)		
	deepracer:UserToken (p. 456)		deepracer:MultiUser (p. 456)		
ListLeaderboards [permission only]	Grants permission to list all the available leaderboards	Read		deepracer:UserToken (p. 456)	deepracer:MultiUser (p. 456)
ListModels [permission only]	Grants permission to list all existing DeepRacer models	Read		deepracer:UserToken (p. 456)	deepracer:MultiUser (p. 456)
ListPrivateLeaderboards [permission only]	Grants permission to retrieve participant information about private leaderboards	Read	leaderboard* (p. 455)		
	deepracer:UserToken (p. 456)		deepracer:MultiUser (p. 456)		
ListPrivateLeaderboards [permission only]	Grants permission to list all the available private leaderboards	Read		deepracer:UserToken (p. 456)	deepracer:MultiUser (p. 456)
ListSubscribedPrivateLeaderboards [permission only]	Grants permission to list all the subscribed private leaderboards	Read		deepracer:UserToken (p. 456)	deepracer:MultiUser (p. 456)
ListTagsForResource [resource]	Grants permission to lists tag for resource	Read	car (p. 455)		
evaluation_job (p. 455)					
leaderboard (p. 455)					
leaderboard_evaluation_job (p. 455)					
reinforcement_learning_model (p. 455)					

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions	
			training_job (p. 455) aws:ResourceTag/ \${TagKey} (p. 456)		depracer:UserToken (p. 456) depracer:MultiUser (p. 456)	
ListTracks [permission only]	Grants permission to list all DeepRacer tracks	Read				
ListTrainingJobs [permission only]	Grants permission to list a DeepRacer model's training jobs	Read	reinforcement_learning_model* (p. 455)			
					depracer:UserToken (p. 456)	depracer:MultiUser (p. 456)
MigrateModels [permission only]	Grants permission to migrate previous reinforcement learning models for DeepRacer	Write				
PerformLeaderboard [permission only]	Grants permission to performs the Leaderboard operation mentioned in the operation attribute	Write	leaderboard (p. 455)			
					depracer:UserToken (p. 456)	depracer:MultiUser (p. 456)
RemoveLeaderboard [permission only]	Grants permission to remove access for private leaderboard	Write	leaderboard* (p. 455)			
					depracer:UserToken (p. 456)	depracer:MultiUser (p. 456)
SetAlias [permission only]	Grants permission to set the user's alias for submitting a DeepRacer model to leaderboards	Write		depracer:UserToken (p. 456)	depracer:MultiUser (p. 456)	
StartEvaluation [permission only]	Grants permission to evaluate a DeepRacer model in a simulated environment	Write	reinforcement_learning_model* (p. 455)			
				track* (p. 455)		
				aws:RequestTag/ \${TagKey} (p. 456)	aws:TagKeys (p. 456)	depracer:UserToken (p. 456)
					depracer:MultiUser (p. 456)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopEvaluation [permission only]	Grants permission to stop DeepRacer model evaluations	Write	evaluation_job* (p. 455)		
				deepracer:UserToken (p. 456)	deepracer:MultiUser (p. 456)
StopTrainingReinforcementLearningModel [permission only]	Grants permission to stop training a DeepRacer model	Write	reinforcement_learning_model* (p. 455)		
				deepracer:UserToken (p. 456)	deepracer:MultiUser (p. 456)
TagResource	Grants permission to tag a resource	Tagging	car (p. 455)		
evaluation_job (p. 455)					
leaderboard (p. 455)					
leaderboard_evaluation_job (p. 455)					
reinforcement_learning_model (p. 455)					
training_job (p. 455)					
	aws:TagKeys (p. 456)				
	aws:RequestTag/ \${TagKey} (p. 456)				
	aws:ResourceTag/ \${TagKey} (p. 456)				
	deepracer:UserToken (p. 456)				
TestRewardFunction [permission only]	Grants permission to test reward functions for correctness	Write			
UntagResource	Grants permission to untag a resource	Tagging	car (p. 455)		
	evaluation_job (p. 455)				
	leaderboard (p. 455)				
	leaderboard_evaluation_job (p. 455)				
	reinforcement_learning_model (p. 455)				
	training_job (p. 455)				

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys (p. 456) aws:RequestTag/\${TagKey} (p. 456) aws:ResourceTag/\${TagKey} (p. 456) deepracer:UserToken (p. 456) deepracer:MultiUser (p. 456)	
UpdateCar [permission only]	Grants permission to update a DeepRacer car in your garage	Write	car* (p. 455)		
	deepracer:UserToken (p. 456) deepracer:MultiUser (p. 456)				

Resource types defined by AWS DeepRacer

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the [Actions table \(p. 448\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
car	arn:\${Partition}:deepracer:\${Region}: \${Account}:car/\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 456)
evaluation_job	arn:\${Partition}:deepracer:\${Region}: \${Account}: evaluation_job/\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 456)
leaderboard	arn:\${Partition}:deepracer: \${Region}:leaderboard/\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 456)
leaderboard_evaluation_job	arn:\${Partition}:deepracer:\${Region}: \${Account}:leaderboard_evaluation_job/ \${ResourceId}	aws:ResourceTag/\${TagKey} (p. 456)
reinforcement_learning_model	arn:\${Partition}:deepracer:\${Region}: \${Account}:model/reinforcement_learning/ \${ResourceId}	aws:ResourceTag/\${TagKey} (p. 456)
track	arn:\${Partition}:deepracer:\${Region}:::track/ \${ResourceId}	
training_job	arn:\${Partition}:deepracer:\${Region}: \${Account}:training_job/\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 456)

Condition keys for AWS DeepRacer

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

To view the global condition keys that are available to all services, see [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters actions by tag key-value pairs in the request	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters actions by tag key-value pairs attached to the resource	String
<code>aws:TagKeys</code>	Filters actions by tag keys in the request	ArrayOfString
<code>deepracer:MultiUser</code>	Filters access by multiuser flag	Bool
<code>deepracer:UserToken</code>	Filters access by user token in the request	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 \(p. 456\)](#)
- [Resource types defined by Amazon Detective \(p. 459\)](#)
- [Condition keys for Amazon Detective \(p. 459\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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			
CreateGraph	Grants permission to create a behavior graph and begin to aggregate security information	Write		aws:RequestTag/\${TagKey} (p. 459) aws:TagKeys (p. 460)	
CreateMembers	Grants permission to request the membership of one or more accounts in a behavior graph managed by this account	Write	Graph* (p. 459)		
DeleteGraph	Grants permission to delete a behavior graph and stop aggregating security information	Write	Graph* (p. 459)		
DeleteMembers	Grants permission to remove member accounts from a behavior graph managed by this account	Write	Graph* (p. 459)		
DescribeOrganization	Grants permission to view the current configuration related to the Amazon Detective integration with AWS Organizations	Read	Graph* (p. 459)		organizations:DescribeOrganization
DisableOrganization	Grants permission to remove the Amazon Detective delegated administrator account for an organization	Write	Graph* (p. 459)		organizations:DescribeOrganization
DisassociateMember	Grants permission to remove the association of this account with a behavior graph	Write			
EnableOrganization	Grants permission to designate the Amazon Detective delegated administrator account for an organization	Write			iam>CreateServiceLinkedRole organizations:DescribeOrganization organizations:EnableAWSOrganizations organizations:RegisterDelegatedAdministrator
GetFreeTrialEligibility	Grants permission to retrieve a behavior graph's eligibility for a free trial period	Read	Graph* (p. 459)		

Service Authorization Reference
Service Authorization Reference
Amazon Detective

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
[permission only]					
GetGraphIngestState [permission only]	Grants permission to retrieve the data ingestion state of a behavior graph	Read	Graph* (p. 459)		
GetMembers	Grants permission to retrieve details on specified members of a behavior graph	Read	Graph* (p. 459)		
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* (p. 459)		
ListGraphs [permission only]	Grants permission to list behavior graphs managed by this account	List			
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* (p. 459)		
ListOrganizationAdmins [current account]	Grants permission to view the current Amazon Detective delegated administrator account for an organization	List	Graph* (p. 459)		organizations:DescribeOrganization
ListTagsForResource	Grants permission to list the tag values that are assigned to a behavior graph	Read	Graph* (p. 459)		
					aws:ResourceTag/ \${TagKey} (p. 460)
RejectInvitation	Grants permission to reject an invitation to become a member of a behavior graph	Write			
SearchGraph [permission only]	Grants permission to search the data stored in a behavior graph	Read	Graph* (p. 459)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartMonitoringDataIngest	Grants permission to start data ingest for a member account that has a status of ACCEPTED_BUT_DISABLED	Write	Graph* (p. 459)		
TagResource	Grants permission to assign tag values to a behavior graph	Tagging	Graph* (p. 459) aws:TagKeys (p. 460) aws:RequestTag/\${TagKey} (p. 459) aws:ResourceTag/\${TagKey} (p. 460)		
UntagResource	Grants permission to remove tag values from a behavior graph	Tagging	Graph* (p. 459) aws:TagKeys (p. 460)		
UpdateOrganizationConfiguration	Grants permission to update the current configuration related to the Amazon Detective integration with AWS Organizations	Write	Graph* (p. 459)		organizations:DescribeOrganizations

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 \(p. 456\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
Graph	<code>arn:\${Partition}:detective:\${Region}:\${Account}:graph:\${ResourceId}</code>	aws:ResourceTag/\${TagKey} (p. 460)

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 [Available global condition keys](#).

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

Condition keys	Description	Type
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	String

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 \(p. 460\)](#)
- [Resource types defined by AWS Device Farm \(p. 467\)](#)
- [Condition keys for AWS Device Farm \(p. 468\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 467)		
CreateInstanceProfile	Grants permission to create a device instance profile	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateNetworkProfile	Grants permission to create a network profile within a project	Write	project* (p. 467)		
CreateProject	Grants permission to create a project for mobile testing	Write		aws:RequestTag/ \${TagKey} (p. 469) aws:TagKeys (p. 469)	
CreateRemoteAccessSession	Grants permission to start a remote access session to a device instance	Write	device* (p. 468)		
			project* (p. 467)		
			deviceinstance (p. 468)		
			upload (p. 468)		
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* (p. 468)		
CreateUpload	Grants permission to upload a new file or app within a project	Write	project* (p. 467)		
CreateVPCEConfig	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* (p. 468)		
DeleteInstanceProfile	Grants permission to delete a user-generated instance profile	Write	instanceprofile* (p. 468)		
DeleteNetworkProfile	Grants permission to delete a user-generated network profile	Write	networkprofile* (p. 468)		
DeleteProject	Grants permission to delete a mobile testing project	Write	project* (p. 467)		
DeleteRemoteAccessSession	Grants permission to delete a completed remote access session and its results	Write	session* (p. 468)		
DeleteRun	Grants permission to delete a run	Write	run* (p. 468)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTestGridProject	Grants permission to delete a desktop testing project	Write	testgrid-project* (p. 468)		
DeleteUpload	Grants permission to delete a user-uploaded file	Write	upload* (p. 468)		
DeleteVPCEConfiguration	Grants permission to delete an Amazon Virtual Private Cloud (VPC) endpoint configuration	Write	vpceconfiguration* (p. 468)		
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* (p. 468)		
GetDeviceInstance	Grants permission to retrieve the information of a device instance	Read	deviceinstance* (p. 468)		
GetDevicePool	Grants permission to retrieve the information of a device pool	Read	devicepool* (p. 468)		
GetDevicePoolCompatibility	Grants permission to retrieve information about the compatibility of a test and/or app with a device pool	Read	devicepool* (p. 468)		
GetDevicePoolCompatibility			upload (p. 468)		
GetInstanceProfile	Grants permission to retrieve the information of an instance profile	Read	instanceprofile* (p. 468)		
GetJob	Grants permission to retrieve the information of a job	Read	job* (p. 468)		
GetNetworkProfile	Grants permission to retrieve the information of a network profile	Read	networkprofile* (p. 468)		
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* (p. 467)		
GetRemoteAccessSession	Grants permission to retrieve the link to a currently running remote access session	Read	session* (p. 468)		
GetRun	Grants permission to retrieve the information of a run	Read	run* (p. 468)		

Service Authorization Reference
Service Authorization Reference
AWS Device Farm

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSuite	Grants permission to retrieve the information of a testing suite	Read	suite* (p. 468)		
GetTest	Grants permission to retrieve the information of a test case	Read	test* (p. 468)		
GetTestGridProject	Grants permission to retrieve information about a desktop testing project	Read	testgrid-project* (p. 468)		
GetTestGridSession	Grants permission to retrieve the information of a test grid session	Read	testgrid-project (p. 468)		
	testgrid-session (p. 468)				
GetUpload	Grants permission to retrieve the information of an uploaded file	Read	upload* (p. 468)		
GetVPCEConfiguration	Grants permission to retrieve the information of an Amazon Virtual Private Cloud (VPC) endpoint configuration	Read	vpceconfiguration* (p. 468)		
InstallToRemoteDevice	Grants permission to install an application to a device in a remote access session	Write	session* (p. 468)		
	upload* (p. 468)				
ListArtifacts	Grants permission to list the artifacts in a project	List	job (p. 468)		
run (p. 468)					
suite (p. 468)					
test (p. 468)					
ListDeviceInstances	Grants permission to list the information of device instances	List			
ListDevicePools	Grants permission to list the information of device pools	List	project* (p. 467)		
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* (p. 468)		
ListNetworkProfiles	Grants permission to list the information of network profiles within a project	List	project* (p. 467)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions	
ListOfferingPromotions	Grants permission to list the offerings promotions	List				
ListOfferingTransactions	Grants permission to list all 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				
ListProjects	Grants permission to list the information of mobile testing projects for an AWS account	List				
ListRemoteAccessInformation	Grants permission to list the information of currently running remote access sessions	List	project* (p. 467)			
ListRuns	Grants permission to list the information of runs within a project	List	project* (p. 467)			
ListSamples	Grants permission to list the information of samples within a project	List	job* (p. 468)			
ListSuites	Grants permission to list the information of testing suites within a job	List	job* (p. 468)			
ListTagsForResource	Grants permission to list the tags of a resource	List	device (p. 468)			
				deviceinstance (p. 468)		
				devicepool (p. 468)		
				instanceprofile (p. 468)		
				networkprofile (p. 468)		
				project (p. 467)		
				run (p. 468)		
				session (p. 468)		
				testgrid-project (p. 468)		
				testgrid-session (p. 468)		
			vpceconfiguration (p. 468)			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTestGridProjects	Grants permission to list the information of desktop testing projects for an AWS account	List			
ListTestGridSessionActions	Grants permission to list the actions performed during a test grid session	List	testgrid-session* (p. 468)		
ListTestGridSessionArtifacts	Grants permission to list the artifacts generated by a test grid session	List	testgrid-session* (p. 468)		
ListTestGridSessions	Grants permission to list the sessions within a test grid project	List	testgrid-project* (p. 468)		
ListTests	Grants permission to list the information of tests within a testing suite	List	suite* (p. 468)		
ListUniqueProblems	Grants permission to list the information of unique problems within a run	List	run* (p. 468)		
ListUploads	Grants permission to list the information of uploads within a project	List	project* (p. 467)		
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* (p. 467)		
	devicepool (p. 468)				
	upload (p. 468)				
SCENARIO: Device Pool as filter			devicepool* (p. 468)		
	project* (p. 467)				
SCENARIO: Device Selection Configuration as filter			upload (p. 468)		
	project* (p. 467)				
			upload (p. 468)		

Service Authorization Reference
Service Authorization Reference
AWS Device Farm

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopJob	Grants permission to terminate a running job	Write	job* (p. 468)		
StopRemoteAccessSession	Grants permission to terminate a running remote access session	Write	session* (p. 468)		
StopRun	Grants permission to terminate a running test run	Write	run* (p. 468)		
TagResource	Grants permission to add tags to a resource	Tagging	device (p. 468)		
deviceinstance (p. 468)					
devicepool (p. 468)					
instanceprofile (p. 468)					
networkprofile (p. 468)					
project (p. 467)					
run (p. 468)					
session (p. 468)					
testgrid-project (p. 468)					
testgrid-session (p. 468)					
vpceconfiguration (p. 468)					
			aws:RequestTag/\${TagKey} (p. 469)		
			aws:TagKeys (p. 469)		
UntagResource	Grants permission to remove tags from a resource	Tagging	device (p. 468)		
deviceinstance (p. 468)					
devicepool (p. 468)					
instanceprofile (p. 468)					
networkprofile (p. 468)					
project (p. 467)					
run (p. 468)					
session (p. 468)					
testgrid-project (p. 468)					

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			testgrid-session (p. 468)		
			vpceconfiguration (p. 468)		
			aws:TagKeys (p. 469)		
UpdateDeviceInstance	Grants permission to modify an existing device instance	Write	deviceinstance* (p. 468)		
			instanceprofile (p. 468)		
UpdateDevicePool	Grants permission to modify an existing device pool	Write	devicepool* (p. 468)		
UpdateInstanceProfile	Grants permission to modify an existing instance profile	Write	instanceprofile* (p. 468)		
UpdateNetworkProfile	Grants permission to modify an existing network profile	Write	networkprofile* (p. 468)		
UpdateProject	Grants permission to modify an existing mobile testing project	Write	project* (p. 467)		
UpdateTestGridProject	Grants permission to modify an existing desktop testing project	Write	testgrid-project* (p. 468)		ec2:CreateNetworkInterface ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:CreateServiceLinkedRole
UpdateUpload	Grants permission to modify an existing upload	Write	upload* (p. 468)		
UpdateVPCEConfiguration	Grants permission to modify an existing Amazon Virtual Private Cloud (VPC) endpoint configuration	Write	vpceconfiguration* (p. 468)		

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 \(p. 460\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
project	<code>arn:\${Partition}:devicefarm:\${Region}:\${Account}:project:\${ResourceId}</code>	aws:ResourceTag/\${TagKey} (p. 469)

Resource types	ARN	Condition keys
run	arn:\${Partition}:devicefarm:\${Region}: \${Account}:run:\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 469)
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} (p. 469)
deviceinstance	arn:\${Partition}:devicefarm: \${Region}::deviceinstance:\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 469)
session	arn:\${Partition}:devicefarm:\${Region}: \${Account}:session:\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 469)
devicepool	arn:\${Partition}:devicefarm:\${Region}: \${Account}:devicepool:\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 469)
device	arn:\${Partition}:devicefarm: \${Region}::device:\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 469)
instanceprofile	arn:\${Partition}:devicefarm:\${Region}: \${Account}:instanceprofile:\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 469)
vpceconfiguration	arn:\${Partition}:devicefarm:\${Region}: \${Account}:vpceconfiguration:\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 469)
testgrid-project	arn:\${Partition}:devicefarm:\${Region}: \${Account}:testgrid-project:\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 469)
testgrid-session	arn:\${Partition}:devicefarm:\${Region}: \${Account}:testgrid-session:\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 469)

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters actions based on the allowed set of values for each of the tags	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters actions based on tag-value associated with the resource	String
<code>aws:TagKeys</code>	Filters actions based on the presence of mandatory tags 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 \(p. 469\)](#)
- [Resource types defined by Amazon DevOps Guru \(p. 472\)](#)
- [Condition keys for Amazon DevOps Guru \(p. 472\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 472)		sns:GetTopicAttributes sns:SetTopicAttributes
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			
DescribeAccountHealthForTimeRange	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			
DescribeEventSourceDetails	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			
DescribeOrganizationalHealth	Grants permission to view the health of operations in your organization	Read			
DescribeOrganizationalHealthForTimeRange	Grants permission to view the health of operations within a time range in your organization	Read			
DescribeOrganizationalHealthForHealthCloudFormationStack	Grants permission to view the health of operations for Health AWS CloudFormation stack or AWS Services or accounts specified in DevOps Guru in your organization	Read			
DescribeResourceHealthForOperations	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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
ListAnomaliesForInsight	Grants permission to list 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			
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			
PutFeedback	Grants permission to submit a feedback to DevOps Guru	Write			
RemoveNotificationChannel	Grants permission to remove a notification channel from DevOps Guru	Write	topic* (p. 472)		sns:GetTopicAttributes sns:SetTopicAttributes
SearchInsights	Grants permission to search insights in your account	List			
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			
UpdateEventSource	Grants permission to update an event source for DevOps Guru	Write			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateServiceIntegrations	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 \(p. 469\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
topic	<code>arn:\${Partition}:sns:\${Region}:\${Account}: \${TopicName}</code>	

Condition keys for Amazon DevOps Guru

DevOps Guru 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 [Available keys for conditions](#).

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 \(p. 472\)](#)
- [Resource types defined by AWS Direct Connect \(p. 479\)](#)
- [Condition keys for AWS Direct Connect \(p. 480\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptDirectConnectProposal	Grants permission to accept a proposal request to a proposal a virtual private gateway to a Direct Connect gateway	Write	dx-gateway* (p. 480)		
AllocateConnection	Grants permission to create a hosted connection on an interconnect	Write	dxcon* (p. 480)		
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 (p. 480)		
			dxlag (p. 480)		
				aws:RequestTag/\${TagKey} (p. 480)	
AllocatePrivateVirtualInterface	Grants permission to provision a private virtual interface to be owned by a different customer	Write	dxcon (p. 480)		
			dxlag (p. 480)		
				aws:RequestTag/\${TagKey} (p. 480)	
AllocatePublicVirtualInterface	Grants permission to provision a public virtual interface to be owned by a different customer	Write	dxcon (p. 480)		
			dxlag (p. 480)		
				aws:RequestTag/\${TagKey} (p. 480)	
AllocateTransitVirtualInterface	Grants permission to provision a transit virtual interface to be owned by a different customer	Write	dxcon (p. 480)		
			dxlag (p. 480)		
				aws:RequestTag/\${TagKey} (p. 480)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateConnection	Grants permission to associate a connection with a LAG	Write	dxcon* (p. 480)		
	dxlag* (p. 480)				
AssociateHostedConnection	Grants permission to associate a hosted connection and its virtual interfaces with a link aggregation group (LAG) or interconnect	Write	dxcon* (p. 480)		
	dxcon (p. 480)				
	dxlag (p. 480)				
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 (p. 480)		
	dxlag (p. 480)				
AssociateVirtualInterface	Grants permission to associate a virtual interface with a specified link aggregation group (LAG) or connection	Write	dxvif* (p. 480)		
	dxcon (p. 480)				
	dxlag (p. 480)				
ConfirmConnection	Grants permission to confirm the creation of a hosted connection on an interconnect	Write	dxcon* (p. 480)		
ConfirmCustomerTerm	Grants permission to confirm 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* (p. 480)		
ConfirmPublicVirtualInterface	Grants permission to accept ownership of a public virtual interface created by another customer	Write	dxvif* (p. 480)		
ConfirmTransitVirtualInterface	Grants permission to accept ownership of a transit virtual interface created by another customer	Write	dxvif* (p. 480)		
CreateBGPPeer	Grants permission to create a BGP peer on the specified virtual interface	Write	dxvif* (p. 480)		

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 (p. 480)		
			aws:RequestTag/ \${TagKey} (p. 480)	aws:TagKeys (p. 480)	
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			
CreateDirectConnectAssociation	Grants permission to create an association between a Direct Connect gateway and a virtual private gateway	Write	dx-gateway* (p. 480)		
CreateDirectConnectProposal	Grants permission to create a proposal to associate the specified virtual private gateway with the specified Direct Connect gateway	Write	dx-gateway* (p. 480)		
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 (p. 480)		
			aws:RequestTag/ \${TagKey} (p. 480)	aws:TagKeys (p. 480)	
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 (p. 480)		
			aws:RequestTag/ \${TagKey} (p. 480)	aws:TagKeys (p. 480)	
CreatePrivateVirtualInterface	Grants permission to create a new private virtual interface	Write	dxcon (p. 480)		
	dxlag (p. 480)		aws:RequestTag/ \${TagKey} (p. 480)	aws:TagKeys (p. 480)	
CreatePublicVirtualInterface	Grants permission to create a new public virtual interface	Write	dxcon (p. 480)		
	dxlag (p. 480)				

Service Authorization Reference
Service Authorization Reference
AWS Direct Connect

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 480) aws:TagKeys (p. 480)	
CreateTransitVirtualInterface	Grants permission to create a new transit virtual interface	Write	dxcon (p. 480)		
			dxlag (p. 480)		
				aws:RequestTag/ \${TagKey} (p. 480) aws:TagKeys (p. 480)	
DeleteBGPPeer	Grants permission to delete the specified BGP peer on the specified virtual interface with the specified customer address and ASN	Write	dxvif* (p. 480)		
DeleteConnection	Grants permission to delete the connection	Write	dxcon* (p. 480)		
DeleteDirectConnectGateway	Grants permission to delete the specified Direct Connect gateway	Write	dx-gateway* (p. 480)		
DeleteDirectConnectAssociation	Grants permission to delete the association between the specified Direct Connect gateway and virtual private gateway	Write	dx-gateway* (p. 480)		
DeleteDirectConnectAssociationProposal	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* (p. 480)		
DeleteLag	Grants permission to delete the specified link aggregation group (LAG)	Write	dxlag* (p. 480)		
DeleteVirtualInterface	Grants permission to delete a virtual interface	Write	dxvif* (p. 480)		
DescribeConnections	Grants permission to describe the LOA-CFA for a Connection	Read	dxcon* (p. 480)		
DescribeConnections	Grants permission to describe all connections in this region	Read	dxcon (p. 480)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeConnections	Grants permission to describe a list of connections that have been provisioned on the given interconnect	Read	dxcon* (p. 480)		
DescribeCustomerAttachments	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			
DescribeDirectConnectAssociations	Grants permission to describe one or more association proposals for connection between a virtual private gateway and a Direct Connect gateway	Read	dx-gateway (p. 480)		
DescribeDirectConnectAttachments	Grants permission to describe the associations between your Direct Connect gateways and virtual private gateways	Read	dx-gateway (p. 480)		
DescribeDirectConnectGateways	Grants permission to describe the attachments between your Direct Connect gateways and virtual interfaces	Read	dx-gateway (p. 480)		
DescribeDirectConnectGateway	Grants permission to describe all your Direct Connect gateways or only the specified Direct Connect gateway	Read	dx-gateway (p. 480)		
DescribeHostedConnections	Grants permission to describe the hosted connections that have been provisioned on the specified interconnect or link aggregation group (LAG)	Read	dxcon (p. 480)		
			dxlag (p. 480)		
DescribeInterconnectLoaCfa	Grants permission to describe the LOA-CFA for an Interconnect	Read	dxcon* (p. 480)		
DescribeInterconnects	Grants permission to describe a list of interconnects owned by the AWS account	Read	dxcon (p. 480)		
DescribeLags	Grants permission to describe all your link aggregation groups (LAG) or the specified LAG	Read	dxlag (p. 480)		
DescribeLoa	Grants permission to describe the LOA-CFA for a connection, interconnect, or link aggregation group (LAG)	Read	dxcon (p. 480)		
			dxlag (p. 480)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeLocations	Grants permission to describe the list of AWS Direct Connect locations in the current AWS region	Read			
DescribeRouterConfigurations	Grants permission to describe details about the router for a virtual interface	Read	dxvif* (p. 480)		
DescribeTags	Grants permission to describe the tags associated with the specified AWS Direct Connect resources	Read	dxcon (p. 480)		
			dxlag (p. 480)		
			dxvif (p. 480)		
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 (p. 480)		
			dxlag (p. 480)		
			dxvif (p. 480)		
DisassociateConnection	Grants permission to disassociate a connection from a link aggregation group (LAG)	Write	dxcon * (p. 480)		
DisassociateMacSecurityKey	Grants permission to remove the association between a MAC Security (MACsec) security key and an AWS Direct Connect dedicated connection	Write	dxcon (p. 480)		
ListVirtualInterfaceFailoverHistory	Grants permission to list the virtual interface failover test history	List	dxvif * (p. 480)		
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 * (p. 480)		
StopBgpFailoverTest	Grants permission to stop the virtual interface failover test	Write	dxvif * (p. 480)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	dxcon (p. 480)		
	dxlag (p. 480)				
	dxvif (p. 480)				
	aws:RequestTag/ {\$TagKey} (p. 480) aws:TagKeys (p. 480)				
UntagResource	Grants permission to remove one or more tags from the specified AWS Direct Connect resource	Tagging	dxcon (p. 480)		
	dxlag (p. 480)				
	dxvif (p. 480)				
	aws:TagKeys (p. 480)				
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* (p. 480)		
UpdateDirectConnectGateway	Grants permission to update the name of a Direct Connect gateway	Write	dx-gateway* (p. 480)		
UpdateDirectConnectAssociation	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* (p. 480)		
UpdateVirtualInterface	Grants permission to update the specified attributes of the specified virtual private interface	Write	dxvif* (p. 480)		

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 \(p. 472\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 480)
dxlag	arn:\${Partition}:directconnect:\${Region}: \${Account}:dxlag/\${LagId}	aws:ResourceTag/\${TagKey} (p. 480)
dxvif	arn:\${Partition}:directconnect:\${Region}: \${Account}:dxvif/\${VirtualInterfaceId}	aws:ResourceTag/\${TagKey} (p. 480)
dx-gateway	arn:\${Partition}:directconnect:: \${Account}:dx-gateway/ \${DirectConnectGatewayId}	

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 [Available global condition 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	String

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 \(p. 481\)](#)
- [Resource types defined by AWS Directory Service \(p. 488\)](#)
- [Condition keys for AWS Directory Service \(p. 489\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 488)		
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* (p. 488)		ec2:AuthorizeSecurityGroupEntries ec2:AuthorizeSecurityGroupOutgress ec2:DescribeSecurityGroups
AddRegion	Grants permission to add two domain controllers in the specified Region for the specified directory	Write	directory* (p. 488)		
AddTagsToResource	Grants permission to add or overwrite one or more tags for the specified Amazon Directory Services directory	Tagging	directory* (p. 488) aws:RequestTag/ \${TagKey} (p. 489) aws:TagKeys (p. 489)		ec2:CreateTags
AuthorizeApplication [permission only]	Grants permission to authorize an application for your AWS Directory	Write	directory* (p. 488)		
CancelSchemaExtension	Grants permission to cancel an in-progress schema extension to a Microsoft AD directory	Write	directory* (p. 488)		
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} (p. 489)	ec2:AuthorizeSecurityGroup aws:TagKeys (p. 489) ec2>CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterface ec2:DescribeSubnets ec2:DescribeVpcs
CreateAlias	Grants permission to create an alias for a directory and assigns the alias to the directory	Write	directory* (p. 488)		
CreateComputer	Grants permission to create a computer account in the specified directory, and joins the computer to the directory	Write	directory* (p. 488)		
CreateConditionalForwarder	Grants permission to create a conditional forwarder associated with your AWS directory	Write	directory* (p. 488)		
CreateDirectory	Grants permission to create a Simple AD directory	Write		aws:RequestTag/ \${TagKey} (p. 489)	ec2:AuthorizeSecurityGroup aws:TagKeys (p. 489) ec2>CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterface ec2:DescribeSubnets ec2:DescribeVpcs
CreateIdentityProvider [permission only]	Grants permission to create an Identity Provider Directory in the AWS cloud	Write		aws:RequestTag/ \${TagKey} (p. 489)	aws:TagKeys (p. 489)
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* (p. 488)		

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} (p. 489)	ec2:AuthorizeSecurityGroup aws:TagKeys (p. 489) ec2>CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterface ec2:DescribeSubnets ec2:DescribeVpcs
CreateSnapshot	Grants permission to create a snapshot of a Simple AD or Microsoft AD directory in the AWS cloud	Write	directory* (p. 488)		
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* (p. 488)		
DeleteConditionalForwarder	Grants permission to delete a conditional forwarder that has been set up for your AWS directory	Write	directory* (p. 488)		
DeleteDirectory	Grants permission to delete an AWS Directory Service directory	Write	directory* (p. 488)		ec2>DeleteNetworkInterface ec2>DeleteSecurityGroup ec2:DescribeNetworkInterface ec2:RevokeSecurityGroup ec2:RevokeSecurityGroup
DeleteLogSubscription	Grants permission to delete the specified log subscription	Write	directory* (p. 488)		
DeleteSnapshot	Grants permission to delete a directory snapshot	Write	directory* (p. 488)		
DeleteTrust	Grants permission to delete an existing trust relationship between your Microsoft AD in the AWS cloud and an external domain	Write	directory* (p. 488)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeregisterCertificate	Grants permission to delete from the system the certificate that was registered for a secured LDAP connection	Write	directory* (p. 488)		
DeregisterEventTopic	Grants permission to remove the specified directory as a publisher to the specified SNS topic	Write	directory* (p. 488)		
DescribeCertificate	Grants permission to display information about the certificate registered for a secured LDAP connection	Read	directory* (p. 488)		
DescribeClientAuthentication	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* (p. 488)		
DescribeConditionalForwarder	Grants permission to obtain information about the conditional forwarders for this account	Read	directory* (p. 488)		
DescribeDirectory	Grants permission to obtain information about the directories that belong to this account	List			
DescribeDomainController	Grants permission to provide information about any domain controllers in your directory	Read	directory* (p. 488)		
DescribeEventTopic	Grants permission to obtain information about which SNS topics receive status messages from the specified directory	Read	directory* (p. 488)		
DescribeLDAPSSettings	Grants permission to describe the status of LDAP security for the specified directory	Read	directory* (p. 488)		
DescribeRegions	Grants permission to provide information about the Regions that are configured for multi-Region replication	Read	directory* (p. 488)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeSharedDirectories	Grants permission to return the shared directories in your account	Read	directory* (p. 488)		
DescribeSnapshotInformation	Grants permission to obtain information about the directory snapshots that belong to this account	Read			
DescribeTrusts	Grants permission to obtain information about the trust relationships for this account	Read			
DisableClientAuthenticationAlternative	Grants permission to disable alternative client authentication methods for the specified directory	Write	directory* (p. 488)		
DisableLDAPS	Grants permission to deactivate LDAP secure calls for the specified directory	Write	directory* (p. 488)		
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* (p. 488)		
DisableSso	Grants permission to disable single-sign on for a directory	Write	directory* (p. 488)		
EnableClientAuthenticationAlternative	Grants permission to enable alternative client authentication methods for the specified directory	Write	directory* (p. 488)		
EnableLDAPS	Grants permission to activate the switch for the specific directory to always use LDAP secure calls	Write	directory* (p. 488)		
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* (p. 488)		
EnableSso	Grants permission to enable single-sign on for a directory	Write	directory* (p. 488)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAuthorizedApplications [permission only]	Grants permission to retrieve the details of the authorized applications on a directory	Read	directory* (p. 488)		
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* (p. 488)		
ListAuthorizedApplications [permission only]	Grants permission to obtain the AWS SSO applications authorized for a directory	Read	directory* (p. 488)		
ListCertificates	Grants permission to list all the certificates registered for a secured LDAP connection, for the specified directory	List	directory* (p. 488)		
ListIpRoutes	Grants permission to list the address blocks that you have added to a directory	Read	directory* (p. 488)		
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* (p. 488)		
ListTagsForResource	Grants permission to list all tags on an Amazon Directory Services directory	Read	directory* (p. 488)		
RegisterCertificate	Grants permission to register a certificate for secured LDAP connection	Write	directory* (p. 488)		
RegisterEventTopic	Grants permission to associate a directory with an SNS topic	Write	directory* (p. 488)	sns:GetTopicAttributes	
RejectSharedDirectory	Grants permission to reject a directory sharing request that was sent from the directory owner account	Write	directory* (p. 488)		
RemoveIpRoutes	Grants permission to remove IP address blocks from a directory	Write	directory* (p. 488)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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* (p. 488)		
RemoveTagsFromDirectory	Grants permission to remove tags from an Amazon Directory Services directory	Tagging	directory* (p. 488)		ec2:DeleteTags
			aws:RequestTag/ \${TagKey} (p. 489)		aws:TagKeys (p. 489)
ResetUserPassword	Grants permission to reset the password for any user in your AWS Managed Microsoft AD or Simple AD directory	Write	directory* (p. 488)		
RestoreFromSnapshot	Grants permission to restore a directory using an existing directory snapshot	Write	directory* (p. 488)		
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* (p. 488)		
StartSchemaExtension	Grants permission to apply a schema extension to a Microsoft AD directory	Write	directory* (p. 488)		
UnauthorizeApplication [permission only]	Grants permission to authorize an application from your AWS Directory	Write	directory* (p. 488)		
UnshareDirectory	Grants permission to stop the directory sharing between the directory owner and consumer accounts	Write	directory* (p. 488)		
UpdateConditionalForwarder	Grants permission to update a conditional forwarder that has been set up for your AWS directory	Write	directory* (p. 488)		

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* (p. 488)		
UpdateRadius	Grants permission to update the Remote Authentication Dial In User Service (RADIUS) server information for an AD Connector directory	Write	directory* (p. 488)		
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* (p. 488)		
VerifyTrust	Grants permission to verify a trust relationship between your Microsoft AD in the AWS cloud and an external domain	Read	directory* (p. 488)		

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 \(p. 481\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
directory	<code>arn:\${Partition}:ds:\${Region}:\${Account}:directory/\${DirectoryId}</code>	aws:ResourceTag/\${TagKey} (p. 489)

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 [Available global condition keys](#).

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

Actions, resources, and condition keys for Amazon DynamoDB

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

References:

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

Topics

- [Actions defined by Amazon DynamoDB \(p. 489\)](#)
- [Resource types defined by Amazon DynamoDB \(p. 496\)](#)
- [Condition keys for Amazon DynamoDB \(p. 497\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetItem	Grants permission to return the attributes of one or more items from one or more tables	Read	table* (p. 496)	dynamodb:Attributes (p. 497) dynamodb:LeadingKeys (p. 497) dynamodb:ReturnConsumedCapacity (p. 497) dynamodb:Select (p. 497)	
BatchWriteItem	Grants permission to put or delete multiple items in one or more tables	Write	table* (p. 496)	dynamodb:Attributes (p. 497) dynamodb:LeadingKeys (p. 497) dynamodb:ReturnConsumedCapacity (p. 497)	
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* (p. 496)	dynamodb:Attributes (p. 497) dynamodb:LeadingKeys (p. 497) dynamodb:ReturnConsumedCapacity (p. 497) dynamodb:ReturnValues (p. 497)	
CreateBackup	Grants permission to create a backup for an existing table	Write	table* (p. 496)		
CreateGlobalTable	Grants permission to create a global table from an existing table	Write	global-table* (p. 496) table* (p. 496)		
 CreateTable	Grants permission to the CreateTable operation adds a new table to your account	Write	table* (p. 496)		
 CreateTableReplica	Grants permission to add a new replica table	Write	table* (p. 496)		
DeleteBackup	Grants permission to delete an existing backup of a table	Write	backup* (p. 496)		
DeleteItem	Grants permission to deletes a single item in a table by primary key	Write	table* (p. 496)	dynamodb:Attributes (p. 497) dynamodb:EnclosingOperation (p. 497) dynamodb:LeadingKeys (p. 497) dynamodb:ReturnConsumedCapacity (p. 497) dynamodb:ReturnValues (p. 497)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTable	Grants permission to the DeleteTable operation which deletes a table and all of its items	Write	table* (p. 496)		
DeleteTableReplica	Grants permission to delete a replica table and all of its items	Write	table* (p. 496)		
DescribeBackup	Grants permission to describe an existing backup of a table	Read	backup* (p. 496)		
DescribeContinuousBackups	Grants permission to check the status of the backup restore settings on the specified table	Read	table* (p. 496)		
DescribeContributorInsights	Grants permission to describe the contributor insights status and related details for a given table or global secondary index	Read	table* (p. 496)		
			index (p. 496)		
DescribeExport	Grants permission to describe an existing Export of a table	Read	export* (p. 496)		
DescribeGlobalTable	Grants permission to return information about the specified global table	Read	global-table* (p. 496)		
DescribeGlobalTableSettings	Grants permission to return settings information about the specified global table	Read	global-table* (p. 496)		
DescribeKinesisStreamingTables	Grants permission to grant permission to describe the status of Kinesis streaming and related details for a given table	Read	table* (p. 496)		
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	Grants permission to describe capacity more of the Reserved Capacity purchased	Read			
DescribeReservedOfferings	Grants permission to describe 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* (p. 496)		
DescribeTable	Grants permission to return information about the table	Read	table* (p. 496)		
DescribeTableReplicaAutoScaling	Grants permission to describe the Auto Scaling settings across all replicas of the global table	Read	table* (p. 496)		
DescribeTimeToLive	Grants permission to give a description of the Time to Live (TTL) status on the specified table	Read	table* (p. 496)		
DisableKinesisStreamTableReplication	Grants permission to grant permission to stop replication from the DynamoDB table to the Kinesis data stream	Write	table* (p. 496)		
EnableKinesisStreamTableReplication	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* (p. 496)		
ExportTableToPointInTime	Grants permission to initiate an Export of a DynamoDB table to S3	Write	table* (p. 496)		
GetItem	Grants permission to the GetItem operation that returns a set of attributes for the item with the given primary key	Read	table* (p. 496)		
				dynamodb:Attributes (p. 497)	
				dynamodb:EnclosingOperation (p. 497)	
				dynamodb:LeadingKeys (p. 497)	
				dynamodb:ReturnConsumedCapacity (p. 497)	
					dynamodb>Select (p. 497)
GetRecords	Grants permission to retrieve the stream records from a given shard	Read	stream* (p. 496)		
GetShardIterator	Grants permission to return a shard iterator	Read	stream* (p. 496)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListBackups	Grants permission to list backups associated with the account and endpoint	List			
ListContributorInsights	Grants permission to list the <code>ContributorInsightsSummary</code> for all tables and global secondary indexes associated with the current account and endpoint	List			
ListExports	Grants permission to list exports associated with the account and endpoint	List			
ListGlobalTables	Grants permission to list all global tables that have a replica in the specified region	List			
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* (p. 496)		
PartiQLDelete	Grants permission to delete a single item in a table by primary key	Write	table* (p. 496)		
				dynamodb:Attributes (p. 497)	dynamodb:EnclosingOperation (p. 497) dynamodb:LeadingKeys (p. 497) dynamodb:ReturnValues (p. 497)
PartiQLInsert	Grants permission to create a new item, if an item with same primary key does not exist in the table	Write	table* (p. 496)		
				dynamodb:Attributes (p. 497)	dynamodb:EnclosingOperation (p. 497) dynamodb:LeadingKeys (p. 497)
PartiQLSelect	Grants permission to read a set of attributes for items from a table or index	Read	table* (p. 496)		
				index (p. 496)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					dynamodb:Attributes (p. 497) dynamodb:EnclosingOperation (p. 497) dynamodb:FullTableScan (p. 497) dynamodb:LeadingKeys (p. 497) dynamodb:Select (p. 497)
PartiQLUpdate	Grants permission to edit an existing item's attributes	Write	table* (p. 496)		
					dynamodb:Attributes (p. 497) dynamodb:EnclosingOperation (p. 497) dynamodb:LeadingKeys (p. 497) dynamodb:ReturnValues (p. 497)
PurchaseReservedCapacityOfferings	Grants permission to purchases capacity offerings 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* (p. 496)		
					dynamodb:Attributes (p. 497) dynamodb:EnclosingOperation (p. 497) dynamodb:LeadingKeys (p. 497) dynamodb:ReturnConsumedCapacity (p. 497) dynamodb:ReturnValues (p. 497)
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* (p. 496)		
			index (p. 496)		dynamodb:Attributes (p. 497) dynamodb:LeadingKeys (p. 497) dynamodb:ReturnConsumedCapacity (p. 497) dynamodb:ReturnValues (p. 497) dynamodb:Select (p. 497)
RestoreTableFromBackup	Grants permission to create a new table from recovery point on AWS Backup	Write	table* (p. 496)		
					dynamodb:Attributes (p. 497) dynamodb:LeadingKeys (p. 497) dynamodb:ReturnConsumedCapacity (p. 497) dynamodb:ReturnValues (p. 497) dynamodb:Select (p. 497)
RestoreTableFromTable	Grants permission to create a new table from an existing backup	Write	backup* (p. 496)		
			table* (p. 496)		

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* (p. 496)		
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* (p. 496)		
			index (p. 496)		dynamodb:Attributes (p. 497)
					dynamodb:ReturnConsumedCapacity (p. 497)
					dynamodb:ReturnValues (p. 497)
StartAwsBackupJob	Grants permission to create a backup on AWS Backup with advanced features enabled	Write	table* (p. 496)		
TagResource	Grants permission to associate a set of tags with an Amazon DynamoDB resource	Tagging	table* (p. 496)		
UntagResource	Grants permission to remove the association of tags from an Amazon DynamoDB resource	Tagging	table* (p. 496)		
UpdateContinuousBackups	Grants permission to enable or disable continuous backups	Write	table* (p. 496)		
UpdateContributorInsights	Grants permission to update the status for contributor insights for a specific table or global secondary index	Write	table* (p. 496)		
UpdateGlobalTableReplicas	Grants permission to add or remove replicas in the specified global table	Write	global-table* (p. 496)		
			table* (p. 496)		
UpdateGlobalTableSettings	Grants permission to update settings of the specified global table	Write	global-table* (p. 496)		
			table* (p. 496)		
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* (p. 496)		
					dynamodb:Attributes (p. 497)
					dynamodb:EnclosingOperation (p. 497)
					dynamodb:LeadingKeys (p. 497)
					dynamodb:ReturnConsumedCapacity (p. 497)
					dynamodb:ReturnValues (p. 497)

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* (p. 496)		
UpdateTableReplicaAutoScaling	Grants permission to update auto scaling settings on your replica table	Write	table* (p. 496)		
UpdateTimeToLive	Grants permission to enable or disable TTL for the specified table	Write	table* (p. 496)		

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 \(p. 489\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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}	
stream	arn:\${Partition}:dynamodb:\${Region}: \${Account}:table/\${TableName}/stream/ \${StreamLabel}	
table	arn:\${Partition}:dynamodb:\${Region}: \${Account}:table/\${TableName}	
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}	

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 [Available global condition 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
dynamodb:AttributeTable	Filter based on the attribute (field or column) names of the table	String
dynamodb:EnclosingTransaction	Used to block Transactions APIs calls and allow the non-Transaction APIs calls and vice-versa	String
dynamodb:FullTableScan	Used to block full table scan	Bool
dynamodb:LeadingKeys	Filters based on the partition key of the table	String
dynamodb:ReturnConsumedCapacity	Filter based on the ReturnConsumedCapacity parameter of a request. Contains either "TOTAL" or "NONE"	String
dynamodb:ReturnValues	Filter based on the ReturnValues parameter of a request. Contains one of the following: "ALL_OLD", "UPDATED_OLD", "ALL_NEW", "UPDATED_NEW", or "NONE"	String
dynamodb:Select	Filter based on the Select parameter of a Query or Scan request	String

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

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

References:

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

Topics

- [Actions defined by Amazon DynamoDB Accelerator \(DAX\) \(p. 498\)](#)
- [Resource types defined by Amazon DynamoDB Accelerator \(DAX\) \(p. 500\)](#)
- [Condition keys for Amazon DynamoDB Accelerator \(DAX\) \(p. 501\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 501)		
BatchWriteItem	Grants permission to put or delete multiple items in one or more tables	Write	application* (p. 501)		
ConditionCheckItem	Grants permission to the <code>ConditionCheckItem</code> operation that checks the existence of a set of attributes for the item with the given primary key	Read	application* (p. 501)		
CreateCluster	Grants permission to create a DAX cluster	Write	application* (p. 501)		dax>CreateParameterGroup dax>CreateSubnetGroup ec2>CreateNetworkInterface ec2>DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:GetRole iam:PassRole
CreateParameterGroup	Grants permission to create a parameter group	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSubnetGroup	Grants permission to create a subnet group	Write			
DecreaseReplicationFactor	Grants permission to remove one or more nodes from a DAX cluster	Write	application* (p. 501)		
DeleteCluster	Grants permission to delete a previously provisioned DAX cluster	Write	application* (p. 501)		
DeleteItem	Grants permission to delete a single item in a table by primary key	Write	application* (p. 501)		
					dax:EnclosingOperation (p. 501)
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 (p. 501)		
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* (p. 501)		
					dax:EnclosingOperation (p. 501)
IncreaseReplicationFactor	Grants permission to add one or more nodes to a DAX cluster	Write	application* (p. 501)		
ListTags	Grants permission to return a list all of the tags for a DAX cluster	Read	application* (p. 501)		

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* (p. 501)		
				dax:EnclosingOperation (p. 501)	
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* (p. 501)		
RebootNode	Grants permission to reboot a single node of a DAX cluster	Write	application* (p. 501)		
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* (p. 501)		
TagResource	Grants permission to associate a set of tags with a DAX resource	Tagging	application* (p. 501)		
UntagResource	Grants permission to remove the association of tags from a DAX resource	Tagging	application* (p. 501)		
UpdateCluster	Grants permission to modify the settings for a DAX cluster	Write	application* (p. 501)		
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* (p. 501)		
				dax:EnclosingOperation (p. 501)	
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 \(p. 498\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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 [Available global condition 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 \(p. 501\)](#)
- [Resource types defined by Amazon EC2 \(p. 687\)](#)
- [Condition keys for Amazon EC2 \(p. 717\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptReservedInstancesExchangeQuote	Grants permission to accept a convertible Reserved Instance exchange quote	Write		ec2:Region (p. 720)	
AcceptTransitGatewayAttachmentSubnets	Grants permission to accept a request to associate subnets with a transit gateway multicast domain	Write	transit-gateway-attachment	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			transit-gateway-multicast-domain	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
				ec2:Region (p. 720)	
AcceptTransitGatewayPeeringAttachmentRequest	Grants permission to accept a transit gateway peering attachment request	Write	transit-gateway-attachment*	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
				ec2:Region (p. 720)	
AcceptTransitGatewayVpcAttachmentRequest	Grants permission to accept a request to attach a VPC to a transit gateway	Write	transit-gateway-attachment*	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
				ec2:Region (p. 720)	
AcceptVpcEndpointConnectionRequest	Grants permission to accept VPC endpoint connections to your VPC endpoint service	Write	vpc-endpoint-service*	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
				ec2:Region (p. 720)	
AcceptVpcPeeringConnectionRequest	VPC peering connection request	Write	vpc*	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Tenancy (p. 722) ec2:VpcID (p. 722)	

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-peering-connection*	aws:ResourceTag/\${TagKey} (p. 717) (p. 714) ec2:AcceptorVpc (p. 717)	ec2:RequesterVpc (p. 721) ec2:ResourceTag/\${TagKey} (p. 721) ec2:VpcPeeringConnectionID (p. 722)
	ec2:Region (p. 720)				
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 (p. 720)	
AllocateAddress	Grants permission to allocate an Elastic IP address (EIP) to your account	Write	elastic-ip* (p. 687)	aws:RequestTag/ \${TagKey} (p. 717)	aws:CreateTags
	ipv4pool-ec2 (p. 698)		aws:ResourceTag/\${TagKey} (p. 717)	aws:TagKeys (p. 717)	
			ec2:ResourceTag/\${TagKey} (p. 721)		
AllocateHosts	Grants permission to allocate a Dedicated Host to your account	Write	dedicated-host* (p. 690)	aws:RequestTag/ \${TagKey} (p. 717)	aws:CreateTags
	aws:TagKeys (p. 717)				
	ec2:AutoPlacement (p. 718) ec2:AvailabilityZone (p. 718) ec2:HostRecovery (p. 718) ec2:InstanceType (p. 719) ec2:Quantity (p. 720)		aws:TagKeys (p. 717) ec2:AvailabilityZone (p. 718) ec2:HostRecovery (p. 718) ec2:InstanceType (p. 719) ec2:Quantity (p. 720)		
AllocateIpamPoolCidr	Grants permission to allocate a CIDR from an Amazon VPC IP Address Manager (IPAM) pool	Write	ipam-pool* (p. 697)	aws:ResourceTag/\${TagKey} (p. 721)	aws:CreateTags
			ec2:Region (p. 720)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ApplySecurityGroupToTargetAssociation	Grants permission to apply a security group to the association between a Client VPN endpoint and a target network	Write	client-vpn-endpoint* (p. 714) security-group* (p. 70) vpc* (p. 714)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ClientRootCertificateChainArn (p. 721) ec2:CloudwatchLogGroupArn (p. 718) ec2:CloudwatchLogStreamArn (p. 718) ec2:DirectoryArn (p. 718) ec2:ResourceTag/\${TagKey} (p. 721) ec2:SamlProviderArn (p. 721) ec2:ServerCertificateArn (p. 721)	
			aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721) ec2:SecurityGroupID (p. 721)		
			aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721) ec2:VpcID (p. 722)		
			ec2:Region (p. 720)		
AssignIpv6Addresses	Grants permission to assign one or more IPv6 addresses to a network interface	Write	network-interface* (p. 70) ec2:AvailabilityZone (p. 718) ec2:NetworkInterfaceID (p. 719) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Subnet (p. 721) ec2:Vpc (p. 722)	aws:ResourceTag/\${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:NetworkInterfaceID (p. 719) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Subnet (p. 721) ec2:Vpc (p. 722)	ec2:Region (p. 720)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

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* (p. 705)	aws:ResourceTag/\${TagKey} (p. 717)	
	ec2:AvailabilityZone (p. 718)			ec2:NetworkInterfaceID (p. 719)	
				ec2:ResourceTag/\${TagKey} (p. 721)	ec2:Subnet (p. 721)
				ec2:Vpc (p. 722)	
	Grants permission to associate an Elastic IP address (EIP) with an instance or a network interface	Write	elastic-ip (p. 687)	aws:ResourceTag/\${TagKey} (p. 717)	ec2:AllocationId (p. 717)
				ec2:Domain (p. 718)	ec2:PublicIpAddress (p. 720)
				ec2:ResourceTag/\${TagKey} (p. 721)	

Service Authorization Reference
 Service Authorization Reference
 Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance (p. 606);ResourceTag/\${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceAutoRecovery (p. 719) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceMetadataTags (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:PlacementGroup (p. 720) ec2:ProductCode (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)		
		network-interface (p. 719)	aws:ResourceTag/\${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:NetworkInterfaceID (p. 719) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Subnet (p. 721) ec2:Vpc (p. 722)		ec2:Region (p. 720)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

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* (p. 689) subnet* (p. 709)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ClientRootCertificateChainArn (p. 718) ec2:CloudwatchLogGroupArn (p. 718) ec2:CloudwatchLogStreamArn (p. 718) ec2:DirectoryArn (p. 718) ec2:ResourceTag/\${TagKey} (p. 721) ec2:SamlProviderArn (p. 721) ec2:ServerCertificateArn (p. 721)	
	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721) ec2:SubnetID (p. 722)				
	ec2:Region (p. 720)				
AssociateDhcpOptions	Grants permission to associate and disassociate a set of DHCP options with a VPC	Write	dhcp-options* (p. 689)	aws:ResourceTag/\${TagKey} (p. 717) ec2:DhcpOptionsID (p. 718) ec2:ResourceTag/\${TagKey} (p. 721)	
	vpc* (p. 714)		aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Tenancy (p. 722) ec2:VpcID (p. 722)		
			ec2:Region (p. 720)		
AssociateEnclaveCACertificate	Grants permission to associate an ACM certificate with an IAM role to be used in an EC2 Enclave	Write	certificate* (p. 689)		
	role* (p. 705)				
			ec2:Region (p. 720)		

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* (p. 695) aws:ResourceTag/\${TagKey} (p. 717)	iam:PassRole	ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceAutoRecovery (p. 719) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceMetadataTags (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:NewInstanceProfile (p. 719) ec2:PlacementGroup (p. 720) ec2:ProductCode (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)
AssociateInstanceEventWindow	Grants permission to associate one or more targets with an event window	Write	instance-event-window* (p. 695) aws:ResourceTag/\${TagKey} (p. 717)	ec2:ResourceTag/\${TagKey} (p. 721)	ec2:Region (p. 720)
AssociateRouteTable	Grants permission to associate a subnet or gateway with a route table	Write	route-table* (p. 705) aws:ResourceTag/\${TagKey} (p. 717)	ec2:ResourceTag/\${TagKey} (p. 721)	ec2:RouteTableID (p. 721) ec2:Vpc (p. 722)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			internet-gateway (p. 697) aws:ResourceTag/ \${TagKey} (p. 717)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:InternetGatewayID (p. 719) ec2:ResourceTag/ \${TagKey} (p. 721)
			subnet (p. 709) aws:ResourceTag/ \${TagKey} (p. 717)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:AvailabilityZone (p. 718) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SubnetID (p. 722) ec2:Vpc (p. 722)
			vpn-gateway (p. 747) aws:ResourceTag/ \${TagKey} (p. 717)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:ResourceTag/ \${TagKey} (p. 721)
					ec2:Region (p. 720)
AssociateSubnetCidrBlock	Grants permission to associate a CIDR block with a subnet	Write	subnet* (p. 709) aws:ResourceTag/ \${TagKey} (p. 717)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:AvailabilityZone (p. 718) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SubnetID (p. 722) ec2:Vpc (p. 722)
					ec2:Region (p. 720)
AssociateTransitGatewayAttachments	Grants permission to associate attachments and list of subnets with a transit gateway multicast domain	Write	subnet* (p. 709) aws:ResourceTag/ \${TagKey} (p. 717)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:AvailabilityZone (p. 718) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SubnetID (p. 722) ec2:Vpc (p. 722)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-attachment*	aws:ResourceTag/\${TagKey} (p. 717) (p. 710)	ec2:ResourceTag/\${TagKey} (p. 721)
			transit-gateway-multicast-domain* (p. 710)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
				ec2:Region (p. 720)	
AssociateTransitGatewayAttachmentWithRouteTable	Grants permission to associate a transit gateway attachment with a transit gateway route table	Write	transit-gateway-attachment*	aws:ResourceTag/\${TagKey} (p. 717) (p. 710)	ec2:ResourceTag/\${TagKey} (p. 721)
	transit-gateway-route-table* (p. 710)		aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)		
			ec2:Region (p. 720)		
AssociateTrunkInterfaceWithBranch	Grants permission to associate a branch network interface with a trunk network interface	Write			ec2:Region (p. 720)
AssociateVpcCidrBlockWithVpc	Grants permission to associate a CIDR block with a VPC	Write	vpc* (p. 714)	aws:ResourceTag/\${TagKey} (p. 717) ec2:Ipv4IpamPoolId (p. 719) ec2:Ipv6IpamPoolId (p. 719)	
			ec2:ResourceTag/\${TagKey} (p. 721)		
	ipam-pool (p. 697)		ec2:ResourceTag/\${TagKey} (p. 721)		
	ipv6pool-ec2 (p. 698)		aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)		
			ec2:Region (p. 720)		

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* (p. 695) aws:ResourceTag/ \${TagKey} (p. 717)	ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:PlacementGroup (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721)	ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)
			security-group* (p. 705) aws:ResourceTag/ \${TagKey} (p. 717)	ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SecurityGroupID (p. 721) ec2:Vpc (p. 722)	
			vpc* (p. 714) aws:ResourceTag/ \${TagKey} (p. 717)	ec2:ResourceTag/ \${TagKey} (p. 721) ec2:Tenancy (p. 722) ec2:VpcID (p. 722)	
					ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AttachInternetGateway	Grants permission to attach an Internet gateway to a VPC	Write	internet-gateway* (p. 714) aws:ResourceTag/\${TagKey} (p. 717) ec2:InternetGatewayID (p. 719) ec2:ResourceTag/\${TagKey} (p. 721)		
	vpc* (p. 714) aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Tenancy (p. 722) ec2:VpcID (p. 722)				
			ec2:Region (p. 720)		
AttachNetworkInterface	Grants permission to attach a network interface to an instance	Write	instance* (p. 696) aws:ResourceTag/\${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceAutoRecovery (p. 719) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceMetadataTags (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:PlacementGroup (p. 720) ec2:ProductCode (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-interface* (p. 705)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:AvailabilityZone (p. 718) ec2:NetworkInterfaceID (p. 719) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:Subnet (p. 721) ec2:Vpc (p. 722)
					ec2:Region (p. 720)
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* (p. 696)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:PlacementGroup (p. 720) ec2:ProductCode (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume* (p. 714) aws:ResourceTag/ \${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:Encrypted (p. 718) ec2:ParentSnapshot (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:VolumeID (p. 722) ec2:VolumeIops (p. 722) ec2:VolumeSize (p. 722) ec2:VolumeThroughput (p. 722) ec2:VolumeType (p. 722)		ec2:Region (p. 720)
AttachVpnGateway	Grants permission to attach a virtual private gateway to a VPC	Write	vpc* (p. 714) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:Tenancy (p. 722) ec2:VpcID (p. 722)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)	ec2:Region (p. 720)
			vpn-gateway* (p. 714) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions	
AuthorizeClientVpnInbound	Grants permission to add an authorization rule to a Client VPN endpoint	Write	client-vpn-endpoint* (p. 718)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ClientRootCertificateChainArn (p. 718) ec2:CloudwatchLogGroupArn (p. 718) ec2:CloudwatchLogStreamArn (p. 718) ec2:DirectoryArn (p. 718) ec2:ResourceTag/\${TagKey} (p. 721) ec2:SamlProviderArn (p. 721) ec2:ServerCertificateArn (p. 721)	ec2:Region (p. 720)	
AuthorizeSecurityGroupInbound	Grants permission to add one or more inbound rules to a VPC security group	Write	security-group* (p. 705)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721) ec2:SecurityGroupID (p. 721) ec2:Vpc (p. 722)	ec2:CreateTags	
			security-group-rule* (p. 706)	aws:RequestTag/\${TagKey} (p. 717) aws:TagKeys (p. 717)	ec2:Region (p. 720)	
AuthorizeSecurityGroupInbound	Grants permission to add one or more inbound rules to a security group	Write	security-group* (p. 705)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721) ec2:SecurityGroupID (p. 721) ec2:Vpc (p. 722)	ec2:CreateTags	
			security-group-rule* (p. 706)	aws:RequestTag/\${TagKey} (p. 717) aws:TagKeys (p. 717)	ec2:Region (p. 720)	
BundleInstance	Grants permission to bundle an instance store-backed Windows instance	Write			ec2:Region (p. 720)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelBundleTask	Grants permission to cancel a bundling operation	Write		ec2:Region (p. 720)	
CancelCapacityReservation	Grants permission to cancel a Capacity Reservation and release the reserved capacity	Write	capacity-reservation* (\${TagKey} (p. 717)) ec2:CapacityReservationFleet (p. 718)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)	ec2:Region (p. 720)
CancelCapacityReservations	Grants permission to cancel one or more Capacity Reservation Fleets	Write	capacity-reservation-fleet* (p. 688)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)	ec2:Region (p. 720)
CancelConversionTask	Grants permission to cancel an active conversion task	Write		ec2:Region (p. 720)	
CancelExportTask	Grants permission to cancel an active export task	Write	export-image-task (p. 692)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)	
			export-instance-task (p. 692)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)	
				ec2:Region (p. 720)	
CancelImportTask	Grants permission to cancel an in-process import virtual machine or import snapshot task	Write	import-image-task (p. 694)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)	
			import-snapshot-task (p. 694)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)	
				ec2:Region (p. 720)	
CancelReservedInstances	Grants permission to cancel a Reserved Instance listing on the Reserved Instance Marketplace	Write		ec2:Region (p. 720)	

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* (p. 708)	aws:ResourceTag/{\${TagKey}} (p. 717) ec2:ResourceTag/{\${TagKey}} (p. 721)	
					ec2:Region (p. 720)
CancelSpotInstanceRequests	Grants permission to cancel one or more Spot Instance requests	Write	spot-instances-request* (p. 708)	aws:ResourceTag/{\${TagKey}} (p. 717) ec2:ResourceTag/{\${TagKey}} (p. 721)	
					ec2:Region (p. 720)
ConfirmProductInEntitlements	Grants permission to determine whether an owned product code is associated with an instance	Write			ec2:Region (p. 720)
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* (p. 693)	ec2:Owner (p. 719)	
					ec2:Region (p. 720)
CopyImage	Grants permission to copy an Amazon Machine Image (AMI) from a source Region to the current Region. Resource-level permissions specified for this action apply to the new AMI only. They do not apply to the source AMI	Write	image* (p. 694)	ec2:ImageID (p. 718)	
				ec2:Owner (p. 719)	
					ec2:Region (p. 720)
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 the new snapshot only. They do not apply to the source snapshot	Write	snapshot* (p. 707)	RequestTag/{\${TagKey}} (p. 717)	
				aws:TagKeys (p. 717)	
				ec2:OutpostArn (p. 719)	
				ec2:SnapshotID (p. 721)	
				ec2:SourceOutpostArn (p. 721)	
					ec2:Region (p. 720)
CreateCapacityReservation	Grants permission to create a Capacity Reservation	Write	capacity-reservation* (p. 788)	aws:RequestTag/{\${TagKey}} (p. 717)	
				aws:TagKeys (p. 717)	
					ec2:CapacityReservationFleet (p. 718)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region (p. 720)	
CreateCapacityReservationFleet	Grants permission to create a Capacity Reservation Fleet	Write	capacity-reservation-fleet* (p. 688)	aws:RequestTag/* \${TagKey} (p. 717) aws:TagKeys (p. 717)	aws:RequestTag/* \${TagKey} (p. 717) aws:CreateTags
				ec2:Region (p. 720)	
CreateCarrierGateway	Grants permission to create a carrier gateway and provides CSP connectivity to VPC customers	Write	carrier-gateway* (p. 714)	aws:RequestTag/* \${TagKey} (p. 717) aws:TagKeys (p. 717)	aws:RequestTag/* \${TagKey} (p. 717) aws:CreateTags
			vpc* (p. 714)	aws:ResourceTag/* \${TagKey} (p. 721) ec2:ResourceTag/* \${TagKey} (p. 721)	
				ec2:Tenancy (p. 722)	
				ec2:VpcID (p. 722)	
				ec2:Region (p. 720)	
CreateClientVpnEndpoint	Grants permission to create a Client VPN endpoint	Write	client-vpn-endpoint* (p. 714)	aws:RequestTag/* \${TagKey} (p. 717) aws:TagKeys (p. 717)	aws:RequestTag/* \${TagKey} (p. 717) aws:CreateTags
				ec2:ClientRootCertificateChainArn (p. 721)	
				ec2:CloudwatchLogGroupArn (p. 718)	
				ec2:CloudwatchLogStreamArn (p. 718)	
				ec2:DirectoryArn (p. 718)	
				ec2:SamlProviderArn (p. 721)	
				ec2:ServerCertificateArn (p. 721)	
			security-group (p. 705)	aws:ResourceTag/* \${TagKey} (p. 721) ec2:ResourceTag/* \${TagKey} (p. 721)	aws:ResourceTag/* \${TagKey} (p. 721) ec2:CreateTags
				ec2:SecurityGroupID (p. 721)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc (p. 714)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:VpcID (p. 722)	
					ec2:Region (p. 720)
CreateClientVpnRoute	Grants permission to add a network route to a Client VPN endpoint's route table	Write	client-vpn-endpoint* (p. 714)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ClientRootCertificateChainArn (p. 718) ec2:CloudwatchLogGroupArn (p. 718) ec2:CloudwatchLogStreamArn (p. 718) ec2:DirectoryArn (p. 718) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SamlProviderArn (p. 721) ec2:ServerCertificateArn (p. 721)	
			subnet* (p. 709)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SubnetID (p. 722)	
					ec2:Region (p. 720)
CreateCoipPoolPermission [permission only]	Grants permission to allow a service to access a customer owned IP (CoIP) pool	Write			ec2:Region (p. 720)
CreateCustomerGateway	Grants permission to create a customer gateway, which provides information to AWS about your customer gateway device	Write	customer-gateway* (p. 709)	aws:RequestTags (p. 717) aws:TagKeys (p. 717)	
CreateDefaultSubnet	Grants permission to create a default subnet in a specified Availability Zone in a default VPC	Write			ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDefaultVpc	Grants permission to create a default VPC with a default subnet in each Availability Zone	Write		ec2:Region (p. 720)	
CreateDhcpOptions	Grants permission to create a set of DHCP options for a VPC	Write	dhcp-options* (p. 691)	aws:RequestTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:DhcpOptionsID (p. 718)	ec2:Region (p. 720)
CreateEgressOnlyInternetGateway	Grants permission to create an egress-only internet gateway for a VPC	Write	egress-only-internet-gateway* (p. 691)	aws:RequestTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717)	aws:RequestTag/ \${TagKey} (p. 717) aws:ResourceTag/ \${TagKey} (p. 714) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:Tenancy (p. 722) ec2:VpcID (p. 722)
					ec2:Region (p. 720)
CreateFleet	Grants permission to launch an EC2 Fleet	Write	fleet* (p. 692) instance* (p. 696)	aws:RequestTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717) aws:RequestTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceID (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:PlacementGroup (p. 720) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)	aws:RequestTag/ \${TagKey} (p. 717)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			image (p. 694) aws:ResourceTag/\${TagKey} (p. 717)		ec2:ImageID (p. 718) ec2:ImageType (p. 718) ec2:Owner (p. 719) ec2:Public (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RootDeviceType (p. 721)
			key-pair (p. 699)	aws:ResourceTag/\${TagKey} (p. 717)	ec2:KeyPairName (p. 719) ec2:KeyPairType (p. 719) ec2:ResourceTag/\${TagKey} (p. 721)
			launch-template (p. 703)	aws:ResourceTag/\${TagKey} (p. 717)	ec2:ResourceTag/\${TagKey} (p. 721)
			network-interface (p. 703)	aws:ResourceTag/\${TagKey} (p. 717)	ec2:AssociatePublicIpAddress (p. 717) ec2:AuthorizedService (p. 717) ec2:AvailabilityZone (p. 718) ec2:NetworkInterfaceID (p. 719) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Subnet (p. 721) ec2:Vpc (p. 722)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			placement-group (p. 703)	aws:ResourceTag/\${TagKey} (p. 717) ec2:PlacementGroupName (p. 720) ec2:PlacementGroupStrategy (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)	
			security-group (p. 705)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721) ec2:SecurityGroupID (p. 721) ec2:Vpc (p. 722)	
			snapshot (p. 707)	aws:ResourceTag/\${TagKey} (p. 717) ec2:Owner (p. 719) ec2:ParentVolume (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:SnapshotID (p. 721) ec2:SnapshotTime (p. 721) ec2:VolumeSize (p. 722)	
			subnet (p. 709)	aws:ResourceTag/\${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:ResourceTag/\${TagKey} (p. 721) ec2:SubnetID (p. 722) ec2:Vpc (p. 722)	

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume (p. 712) aws:RequestTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:AvailabilityZone (p. 718) ec2:Encrypted (p. 718) ec2:KmsKeyId (p. 719) ec2:ParentSnapshot (p. 720) ec2:VolumeID (p. 722) ec2:VolumeIops (p. 722) ec2:VolumeSize (p. 722) ec2:VolumeThroughput (p. 722) ec2:VolumeType (p. 722)		
CreateFlowLogs	Grants permission to create one or more flow logs to capture IP traffic for a network interface	Write	vpc-flow-log* (p. 713)	aws:RequestTag/ \${TagKey} (p. 717) iam:PassRole aws:TagKeys (p. 717)	
			network-interface (p. 703)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:NetworkInterfaceID (p. 719) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:Subnet (p. 721) ec2:Vpc (p. 722)	
			subnet (p. 709)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SubnetID (p. 722) ec2:Vpc (p. 722)	

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc (p. 714)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Tenancy (p. 722) ec2:VpcID (p. 722)	
					ec2:Region (p. 720)
CreateFpgaImage	Grants permission to create an Amazon FPGA Image (AFI) from a design checkpoint (DCP)	Write	fpga-image* (p. 694)	aws:RequestTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Owner (p. 719) ec2:Public (p. 720)	ec2/CreateTags
					ec2:Region (p. 720)
CreateImage	Grants permission to create an Amazon EBS-backed AMI from a stopped or running Amazon EBS-backed instance	Write	image* (p. 694)	aws:RequestTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:ImageID (p. 718) ec2:Owner (p. 719)	ec2/CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance* (p. 695) ResourceTag/ \${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceAutoRecovery (p. 719) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceMetadataTags (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:PlacementGroup (p. 720) ec2:ProductCode (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)	RequestTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:OutpostArn (p. 719) ec2:Owner (p. 719) ec2:ParentVolume (p. 720) ec2:SnapshotID (p. 721) ec2:SnapshotTime (p. 721) ec2:SourceOutpostArn (p. 721) ec2:VolumeSize (p. 722)	ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateInstanceEventWindow	Grants permission to create an event window in which scheduled events for the associated Amazon EC2 instances can run	Write	instance-event-window* (p. 695)	aws:RequestTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717)	ec2:Region (p. 720)
CreateInstanceExportTask	Grants permission to export a running or stopped instance to an Amazon S3 bucket	Write	export-instance-task* (p. 692) instance* (p. 696)ResourceTag/ \${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceAutoRecovery (p. 719) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceMetadataTags (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:ProductCode (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722) ec2:Region (p. 720)		
CreateInternetGateway	Grants permission to create an internet gateway for a VPC	Write	internet-gateway* (p. 717)	aws:RequestTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717)	ec2:InternetGatewayID (p. 719) ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateIpam	Grants permission to create an Amazon VPC IP Address Manager (IPAM)	Write	ipam* (p. 697) aws:RequestTag/ \${TagKey} (p. 717) iam:CreateServiceLinkedRole aws:TagKeys (p. 717)		ec2:Region (p. 720)
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* (p. 697) aws:RequestTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717)		ec2:ResourceTag/ \${TagKey} (p. 721)
			ipam-scope* (p. 698) ec2:ResourceTag/ \${TagKey} (p. 721)		ec2:Region (p. 720)
			ipam* (p. 697) ec2:ResourceTag/ \${TagKey} (p. 721)	aws:RequestTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717)	ec2:Region (p. 720)
CreateKeyPair	Grants permission to create a 2048-bit RSA key pair	Write	key-pair* (p. 699) aws:RequestTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:KeyPairType (p. 719)		ec2:Region (p. 720)
CreateLaunchTemplate	Grants permission to create a launch template	Write	launch-template* (p. 699) aws:RequestTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717)		ec2:Region (p. 720)
CreateLaunchTemplateVersion	Grants permission to create a new version of a launch template	Write	launch-template* (p. 699) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		ec2:Region (p. 720)
CreateLocalGatewayRouteTableEntry	Grants permission to create a static route for a local gateway route table	Write	local-gateway-route-table* (p. 700) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway-virtual-interface-group* (p. 704)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
	CreateLocalGatewayRouteTablePermission [permission only]	Write	local-gateway-route-table* (p. 700)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
	CreateLocalGatewayRouteTableVpcAssociation	Write	local-gateway-route-table* (p. 700)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			local-gateway-route-table-vpc-association* (p. 700)	aws:RequestTag/\${TagKey} (p. 717) aws:TagKeys (p. 717)	
			vpc* (p. 714)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Tenancy (p. 722) ec2:VpcID (p. 722)	
	CreateManagedPrefixList	Write	prefix-list* (p. 704)	aws:RequestTag/\${TagKey} (p. 717) aws:TagKeys (p. 717)	
					ec2:Region (p. 720)
	CreateNatGateway	Write	natgateway* (p. 704)	aws:RequestTag/\${TagKey} (p. 717) aws:TagKeys (p. 717)	

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet* (p. 709) aws:ResourceTag/ \${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SubnetID (p. 722) ec2:Vpc (p. 722)		
			elastic- ip (p. 687) aws:ResourceTag/ \${TagKey} (p. 717) ec2:AllocationId (p. 717) ec2:Domain (p. 718) ec2:PublicIpAddress (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:AllocationId (p. 717) ec2:Domain (p. 718) ec2:PublicIpAddress (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721)	ec2:Region (p. 720)
CreateNetworkAcl	Grants permission to create a network ACL in a VPC	Write	network- acl* (p. 701) aws:RequestTe c2:CreateTags aws:TagKeys (p. 717) ec2:NetworkAclID (p. 719)	aws:RequestTe c2:CreateTags aws:TagKeys (p. 717) ec2:NetworkAclID (p. 719)	aws:RequestTe c2:CreateTags aws:TagKeys (p. 717) ec2:NetworkAclID (p. 719)
			vpc* (p. 714) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:Tenancy (p. 722) ec2:VpcID (p. 722)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:Tenancy (p. 722) ec2:VpcID (p. 722)	ec2:Region (p. 720)
CreateNetworkAclEntry	Grants permission to create a numbered entry (a rule) in a network ACL	Write	network- acl* (p. 701) aws:ResourceTag/ \${TagKey} (p. 717) ec2:NetworkAclID (p. 719) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:Vpc (p. 722)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:NetworkAclID (p. 719) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:Vpc (p. 722)	ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateNetworkInsightsScope	Grants permission to create a Network Insights Scope	Write	network-insights-access-scope* (p. 702)	aws:RequestTag/ \${TagKey} (p. 717)	aws:CreateTags aws:TagKeys (p. 717)
			ec2:Region (p. 720)		
CreateNetworkInsightsPath	Grants permission to create a path to analyze for reachability	Write	network-insights-path* (p. 702)	aws:RequestTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717)	aws:CreateTags aws:TagKeys (p. 717)
			instance (p. 696) aws:ResourceTag/ \${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceId (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:PlacementGroup (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)		
			internet-gateway (p. 697) aws:ResourceTag/ \${TagKey} (p. 717)	aws:CreateTags aws:TagKeys (p. 717) ec2:InternetGatewayID (p. 719) ec2:ResourceTag/ \${TagKey} (p. 721)	

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to create a network interface in a subnet	Write	network-interface (p. 713)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:AssociatePublicIpAddress (p. 717) ec2:AuthorizedService (p. 717) ec2:AvailabilityZone (p. 718) ec2:NetworkInterfaceID (p. 719) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:Subnet (p. 721) ec2:Vpc (p. 722)	
			transit-gateway (p. 717)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)	
			vpc-endpoint (p. 713)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)	
			vpc-peering-connection (p. 714)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:AcceptorVpc (p. 717) ec2:RequesterVpc (p. 721) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:VpcPeeringConnectionID (p. 722)	
			vpn-gateway (p. 717)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)	
				ec2:Region (p. 720)	
CreateNetworkInterface			network-interface* (p. 703)	aws:RequestTags/ CreateTags	
				aws:TagKeys (p. 717)	
					ec2:NetworkInterfaceID (p. 719)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet* (p. 709) aws:ResourceTag/ \${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SubnetID (p. 722) ec2:Vpc (p. 722)		
	security- group (p. 705) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SecurityGroupID (p. 721) ec2:Vpc (p. 722)				
				ec2:Region (p. 720)	
CreateNetworkInterfacePermission	Grants permission to create a permission for an AWS-authorized user to perform certain operations on a network interface	Permissions	network- managementinterface* (p. 705) aws:ResourceTag/ \${TagKey} (p. 717) ec2:AuthorizedService (p. 717) ec2:AuthorizedUser (p. 718) ec2:AvailabilityZone (p. 718) ec2:NetworkInterfaceID (p. 719) ec2:Permission (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:Subnet (p. 721) ec2:Vpc (p. 722)		aws:ResourceTag/ \${TagKey} (p. 717) ec2:Region (p. 720)
CreatePlacementGroup	Grants permission to create a placement group	Write	placement- group* (p. 705) aws:RequestTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:PlacementGroupName (p. 720) ec2:PlacementGroupStrategy (p. 720)		aws:RequestTag/ \${TagKey} (p. 717) ec2:Region (p. 720)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	network-insights-access-scope* (p. 702)	aws:RequestTag/\${TagKey} (p. 717)	ec2:CreateTags aws:TagKeys (p. 717)
					ec2:Region (p. 720)
CreateReplaceRootVolumeTask	Grants permission to create a root volume replacement task	Write	instance* (p. 696) resource* (p. 696) aws:RequestTag/\${TagKey} (p. 717)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:CreateTags aws:TagKeys (p. 717) ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceAutoRecovery (p. 719) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceMetadataTags (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:PlacementGroup (p. 720) ec2:ProductCode (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)
			replace-root-volume-task* (p. 704)	aws:RequestTag/\${TagKey} (p. 717)	aws:TagKeys (p. 717)
			volume* (p. 712)	aws:RequestTag/\${TagKey} (p. 717)	aws:TagKeys (p. 717) ec2:VolumeID (p. 722)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot (p. 207) aws:ResourceTag/ \${TagKey} (p. 717) ec2:Owner (p. 719) ec2:ParentVolume (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SnapshotID (p. 721) ec2:SnapshotTime (p. 721) ec2:VolumeSize (p. 722)		
				ec2:Region (p. 720)	
CreateReservedInstancesOffering	Grants permission to create a listing for Standard Reserved Instances to be sold in the Reserved Instance Marketplace	Write			ec2:Region (p. 720)
CreateRestoreImageTask	Grants permission to start a task that restores an AMI from an S3 object previously created by using CreateStoreImageTask	Write	image* (p. 694) aws:RequestTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:ImageID (p. 718) ec2:Owner (p. 719)		ec2:Region (p. 720)
CreateRoute	Grants permission to create a route in a VPC route table	Write	route-table* (p. 705) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RouteTableID (p. 721) ec2:Vpc (p. 722)		aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RouteTableID (p. 721) ec2:Vpc (p. 722)
CreateRouteTable	Grants permission to create a route table for a VPC	Write	route-table* (p. 705) aws:RequestTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:RouteTableID (p. 721)		aws:RequestTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:RouteTableID (p. 721)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc* (p. 714)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Tenancy (p. 722) ec2:VpcID (p. 722)	aws:RequestTag/ec2/CreateTags ec2:Region (p. 720)
CreateSecurityGroup	Grants permission to create a security group	Write	security-group* (p. 70) vpc (p. 714)	aws:RequestTag/ec2/CreateTags aws:TagKeys (p. 717) ec2:SecurityGroupID (p. 721)	aws:RequestTag/ec2/CreateTags ec2:Region (p. 720)
CreateSnapshot	Grants permission to create a snapshot of an EBS volume and store it in Amazon S3	Write	snapshot* (p. 70) vpc (p. 714)	aws:RequestTag/ec2/CreateTags aws:TagKeys (p. 717) ec2:OutpostArn (p. 719) ec2:ParentVolume (p. 720) ec2:SnapshotID (p. 721) ec2:SourceOutpostArn (p. 721) ec2:VolumeSize (p. 722)	aws:RequestTag/ec2/CreateTags ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume* (p. 712) aws:ResourceTag/ \${TagKey} (p. 717) ec2:Encrypted (p. 718) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:VolumeID (p. 722) ec2:VolumeIops (p. 722) ec2:VolumeSize (p. 722) ec2:VolumeThroughput (p. 722) ec2:VolumeType (p. 722)		ec2:Region (p. 720)
CreateSnapshots	Grants permission to create crash-consistent snapshots of multiple EBS volumes and store them in Amazon S3	Write	instance* (p. 696) aws:ResourceTag/ \${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceId (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:PlacementGroup (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)	snapshot* (p. 707) aws:RequestTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:OutpostArn (p. 719) ec2:ParentVolume (p. 720) ec2:SnapshotID (p. 721) ec2:SourceOutpostArn (p. 721) ec2:VolumeSize (p. 722)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume* (p. 712) aws:ResourceTag/ \${TagKey} (p. 717) ec2:Encrypted (p. 718) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:VolumeID (p. 722) ec2:VolumeIops (p. 722) ec2:VolumeSize (p. 722) ec2:VolumeThroughput (p. 722) ec2:VolumeType (p. 722)		ec2:Region (p. 720)
CreateSpotDatafeedEndpoint	Grants permission to create a data feed for Spot Instances to view Spot Instance usage logs	Write			ec2:Region (p. 720)
CreateStoreImage	Grants permission to store an AMI as a single object in an S3 bucket	Write	image* (p. 694) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ImageID (p. 718) ec2:ImageType (p. 718) ec2:Owner (p. 719) ec2:Public (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RootDeviceType (p. 721)		ec2:Region (p. 720)
CreateSubnet	Grants permission to create a subnet in a VPC	Write	subnet* (p. 709) aws:RequestTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:SubnetID (p. 722)		

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc* (p. 714)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:Tenancy (p. 722) ec2:VpcID (p. 722)	
			ec2:Region (p. 720)		
CreateSubnetCidrReservation	Grants permission to create a Subnet CIDR reservation	Write			ec2:Region (p. 720)
CreateTags	Grants permission to add or overwrite one or more tags for Amazon EC2 resources	Tagging	capacity-reservation (p. 688)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)	
capacity-reservation-fleet (p. 688)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)				
client-vpn-endpoint (p. 690)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ClientRootCertificateChainArn (p. 718) ec2:CloudwatchLogGroupArn (p. 718) ec2:CloudwatchLogStreamArn (p. 718) ec2:DirectoryArn (p. 718) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SamlProviderArn (p. 721) ec2:ServerCertificateArn (p. 721)				
customer-gateway (p. 690)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)				

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			dedicated-host (p. 690)	aws:ResourceTag/\${TagKey} (p. 717) ec2:AutoPlacement (p. 718) ec2:AvailabilityZone (p. 718) ec2:HostRecovery (p. 718) ec2:InstanceType (p. 719) ec2:Quantity (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)	
			dhcp-options (p. 690)	aws:ResourceTag/\${TagKey} (p. 717) ec2:DhcpOptionsID (p. 718) ec2:ResourceTag/\${TagKey} (p. 721)	
			egress-only-internet-gateway (p. 691)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			elastic-gpu (p. 691)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ElasticGpuType (p. 718) ec2:ResourceTag/\${TagKey} (p. 721)	
			elastic-ip (p. 687)	aws:ResourceTag/\${TagKey} (p. 717) ec2:AllocationId (p. 717) ec2:Domain (p. 718) ec2:PublicIpAddress (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)	
			export-image-task (p. 692)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			export-instance-task (p. 692)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			fleet (p. 692)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			fpga-image (p. 693)	aws:ResourceTag/\${TagKey} (p. 717) ec2:Owner (p. 719) ec2:Public (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)	
			host-reservation (p. 693)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			image (p. 694)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ImageID (p. 718) ec2:ImageType (p. 718) ec2:Owner (p. 719) ec2:Public (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RootDeviceType (p. 721)	
			import-image-task (p. 694)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			import-snapshot-task (p. 694)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance (p. 696) :ResourceTag/ \${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceAutoRecovery (p. 719) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceMetadataTags (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:PlacementGroup (p. 720) ec2:ProductCode (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)	
			internet-gateway (p. 697) :ResourceTag/ \${TagKey} (p. 717)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:InternetGatewayID (p. 719)	
			ipam (p. 697) :ResourceTag/ \${TagKey} (p. 721)		
			ipam-pool (p. 697) :ResourceTag/ \${TagKey} (p. 721)	ec2:ResourceTag/ \${TagKey} (p. 721)	

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-scope (p. 698)	ec2:ResourceTag/ \${TagKey} (p. 721)	
			ipv4pool-ec2 (p. 698)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:ResourceTag/ \${TagKey} (p. 721)
			ipv6pool-ec2 (p. 698)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:ResourceTag/ \${TagKey} (p. 721)
			key-pair (p. 699)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:KeyPairName (p. 719)
			launch-template (p. 699)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:ResourceTag/ \${TagKey} (p. 721)
			local-gateway (p. 700)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:ResourceTag/ \${TagKey} (p. 721)
			local-gateway-route-table (p. 700)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:ResourceTag/ \${TagKey} (p. 721)
			local-gateway-route-table-virtual-interface-group-association (p. 700)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:ResourceTag/ \${TagKey} (p. 721)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway-route-table-vpc-association (p. 702)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			local-gateway-virtual-interface (p. 702)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			local-gateway-virtual-interface-group (p. 701)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			natgateway (p. 702)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			network-acl (p. 701)	aws:ResourceTag/\${TagKey} (p. 717) ec2:NetworkAclID (p. 719) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Vpc (p. 722)	
			network-insights-access-scope (p. 702)	ec2:ResourceTag/\${TagKey} (p. 721)	
			network-insights-access-scope-analysis (p. 702)	ec2:ResourceTag/\${TagKey} (p. 721)	

Service Authorization Reference
 Service Authorization Reference
 Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-interface (p. 703)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:AssociatePublicIpAddress (p. 717) ec2:AuthorizedService (p. 717) ec2:AuthorizedUser (p. 718) ec2:AvailabilityZone (p. 718) ec2:NetworkInterfaceID (p. 719) ec2:Permission (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:Subnet (p. 721) ec2:Vpc (p. 722)
			placement-group (p. 703)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:PlacementGroupName (p. 720) ec2:PlacementGroupStrategy (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721)
	prefix-list (p. 704)			aws:ResourceTag/ \${TagKey} (p. 717)	ec2:ResourceTag/ \${TagKey} (p. 721)
	replace-root-volume-task (p. 704)		aws:ResourceTag/ \${TagKey} (p. 717)	ec2:ResourceTag/ \${TagKey} (p. 721)	

Service Authorization Reference
 Service Authorization Reference
 Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			reserved-instances (p. 704)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:AvailabilityZone (p. 718) ec2:InstanceType (p. 719) ec2:ReservedInstancesOfferingType (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:Tenancy (p. 722)
			route-table (p. 705)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RouteTableID (p. 721) ec2:Vpc (p. 722)
			security-group (p. 705)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SecurityGroupID (p. 721) ec2:Vpc (p. 722)
			security-group-rule (p. 706)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:ResourceTag/ \${TagKey} (p. 721)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot (p. 207) aws:ResourceTag/ \${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:Encrypted (p. 718) ec2:Owner (p. 719) ec2:ParentVolume (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SnapshotID (p. 721) ec2:SnapshotTime (p. 721) ec2:VolumeSize (p. 722)		
	spot-fleet-request (p. 708)		aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		
	spot-instances-request (p. 708)		aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		
	subnet (p. 708)		aws:ResourceTag/ \${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SubnetID (p. 722) ec2:Vpc (p. 722)		
	subnet-cidr-reservation (p. 708)		aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		
	traffic-mirror-filter (p. 709)		aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			traffic-mirror-session (p. 710)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			traffic-mirror-target (p. 710)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			transit-gateway (p. 711)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			transit-gateway-attachment (p. 710)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			transit-gateway-connect-peer (p. 711)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			transit-gateway-multicast-domain (p. 712)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			transit-gateway-route-table (p. 712)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume (p. 712) aws:ResourceTag/ \${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:Encrypted (p. 718) ec2:ParentSnapshot (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:VolumeID (p. 722) ec2:VolumeIops (p. 722) ec2:VolumeSize (p. 722) ec2:VolumeThroughput (p. 722) ec2:VolumeType (p. 722)		
		vpc (p. 714)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:Tenancy (p. 722) ec2:VpcID (p. 722)		
		vpc- endpoint (p. 715)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		
		vpc- endpoint- service (p. 713)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:VpceServicePrivateDnsName (p. 722)		
		vpc-flow- log (p. 713)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-peering-connection (p. 714)	aws:ResourceTag/\${TagKey} (p. 717) ec2:AcceptorVpc (p. 717) ec2:RequesterVpc (p. 721) ec2:ResourceTag/\${TagKey} (p. 721) ec2:VpcPeeringConnectionID (p. 722)	
	vpn-connection (p. 716)	aws:ResourceTag/\${TagKey} (p. 717) ec2:AuthenticationType (p. 717) ec2:DPDTimeoutSeconds (p. 718) ec2:GatewayType (p. 718) ec2:IKEVersions (p. 718) ec2:InsideTunnelCidr (p. 718) ec2:InsideTunnelIpv6Cidr (p. 718) ec2:Phase1DHGroup (p. 720) ec2:Phase1EncryptionAlgorithms (p. 720) ec2:Phase1IntegrityAlgorithms (p. 720) ec2:Phase1LifetimeSeconds (p. 720) ec2:Phase2DHGroup (p. 720) ec2:Phase2EncryptionAlgorithms (p. 720) ec2:Phase2IntegrityAlgorithms (p. 720) ec2:Phase2LifetimeSeconds (p. 720) ec2:PreSharedKeys (p. 720) ec2:RekeyFuzzPercentage (p. 721) ec2:RekeyMarginTimeSeconds (p. 721) ec2:ReplayWindowSizePackets (p. 721) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RoutingType (p. 721)			

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpn-gateway (p. 717)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	ec2:CreateAction (p. 718) ec2:Region (p. 720)
	Grants permission to create a traffic mirror filter	Write	traffic-mirror-filter* (p. 709)	aws:RequestTag/\${TagKey} (p. 717) aws:TagKeys (p. 717)	ec2:Region (p. 720)
	Grants permission to create a traffic mirror filter rule	Write	traffic-mirror-filter* (p. 709)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	ec2:Region (p. 720)
	Grants permission to create a traffic mirror session	Write	network-interface* (p. 705)	aws:ResourceTag/\${TagKey} (p. 717) ec2:NetworkInterfaceID (p. 719)	ec2:CreateTags (p. 715) ec2:Region (p. 720)
			traffic-mirror-filter* (p. 709)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	aws:RequestTag/\${TagKey} (p. 717) aws:TagKeys (p. 717)
			traffic-mirror-session* (p. 710)	aws:ResourceTag/\${TagKey} (p. 717)	aws:RequestTag/\${TagKey} (p. 717) aws:TagKeys (p. 717)
			traffic-mirror-target* (p. 710)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	aws:RequestTag/\${TagKey} (p. 717) aws:TagKeys (p. 717)
	Grants permission to create a traffic mirror target	Write	traffic-mirror-target* (p. 710)	aws:ResourceTag/\${TagKey} (p. 717)	aws:RequestTag/\${TagKey} (p. 717) aws:TagKeys (p. 717)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-interface (p. 703) aws:ResourceTag/ \${TagKey} (p. 717) ec2:NetworkInterfaceID (p. 719) ec2:ResourceTag/ \${TagKey} (p. 721)		
			vpc-endpoint (p. 703) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:VpceServiceName (p. 722) ec2:VpceServiceOwner (p. 722)		
					ec2:Region (p. 720)
CreateTransitGateway	Grants permission to create a transit gateway	Write	transit-gateway* (p. 703) aws:RequestTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717)		aws:RequestTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717)
					ec2:Region (p. 720)
CreateTransitGatewayAttachment	Grants permission to create a Connect attachment from a specified transit gateway attachment	Write	transit-gateway-attachment* (p. 710) aws:RequestTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717)		aws:RequestTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717)
					ec2:Region (p. 720)
CreateTransitGatewayConnectPeer	Grants permission to create a Connect peer between a transit gateway and an appliance	Write	transit-gateway-attachment* (p. 710) aws:RequestTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		aws:RequestTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717)
					ec2:Region (p. 720)
CreateTransitGatewayMulticastDomain	Grants permission to create a multicast domain for a transit gateway	Write	transit-gateway* (p. 703) aws:RequestTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		aws:RequestTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-multicast-domain* (p. 710) aws:TagKeys (p. 717)	aws:RequestTag/\${TagKey} (p. 717)	
	Grants permission to request transit gateway peering attachment between a requester and accepter transit gateway	Write	transit-gateway* (p. 710) aws:ResourceTag/\${TagKey} (p. 717)	aws:RequestTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	ec2:CreateTags
			transit-gateway-attachment* (p. 710) aws:TagKeys (p. 717)	aws:RequestTag/\${TagKey} (p. 717)	
	Grants permission to create transit gateway prefix list reference	Write	prefix-list* (p. 704)	aws:ResourceTag/\${TagKey} (p. 717)	
			transit-gateway-route-table* (p. 710)	aws:ResourceTag/\${TagKey} (p. 717)	ec2:ResourceTag/\${TagKey} (p. 721)
			transit-gateway-attachment (p. 710)	aws:ResourceTag/\${TagKey} (p. 717)	ec2:ResourceTag/\${TagKey} (p. 721)
					ec2:Region (p. 720)
	Grants permission to create a static route for a transit gateway route table	Write	transit-gateway-route-table* (p. 710)	aws:ResourceTag/\${TagKey} (p. 717)	ec2:ResourceTag/\${TagKey} (p. 721)
			transit-gateway-attachment (p. 710)	aws:ResourceTag/\${TagKey} (p. 717)	ec2:ResourceTag/\${TagKey} (p. 721)
					ec2:Region (p. 720)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTransitGatewayRouteTable	Grants permission to create a transit gateway route table for a transit gateway	Write	transit-gateway* (p. 710)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:CreateTags
			transit-gateway-route-table* (p. 710)	aws:RequestTag/ \${TagKey} (p. 717)	aws:TagKeys (p. 717)
					ec2:Region (p. 720)
CreateTransitGatewayVpcAttachment	Grants permission to attach a VPC to a transit gateway	Write	transit-gateway* (p. 710)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:CreateTags
			transit-gateway-attachment* (p. 710)	aws:RequestTag/ \${TagKey} (p. 717)	aws:TagKeys (p. 717)
			vpc* (p. 714)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:ResourceTag/ \${TagKey} (p. 721)
			subnet (p. 709)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:AvailabilityZone (p. 718)
					ec2:ResourceTag/ \${TagKey} (p. 721)
				ec2:SubnetID (p. 722)	ec2:Vpc (p. 722)
					ec2:Region (p. 720)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateVolume	Grants permission to create an EBS volume	Write	volume* (p. 712) aws:RequestTag/ \${TagKey} (p. 717)	aws:TagKeys (p. 717)	ec2:AvailabilityZone (p. 718) ec2:Encrypted (p. 718) ec2:KmsKeyId (p. 719) ec2:ParentSnapshot (p. 720) ec2:VolumeID (p. 722) ec2:VolumeIops (p. 722) ec2:VolumeSize (p. 722) ec2:VolumeThroughput (p. 722) ec2:VolumeType (p. 722)
					ec2:Region (p. 720)
CreateVpc	Grants permission to create a VPC with a specified CIDR block	Write	vpc* (p. 714) aws:RequestTag/ \${TagKey} (p. 717)	aws:TagKeys (p. 717)	ec2:Ipv4IpamPoolId (p. 719) ec2:Ipv6IpamPoolId (p. 719) ec2:VpcID (p. 722)
			ipam- pool (p. 697)	ec2:ResourceTag/ \${TagKey} (p. 721)	
			ipv6pool- ec2 (p. 698)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)	
					ec2:Region (p. 720)
CreateVpcEndpoint	Grants permission to create a VPC endpoint for an AWS service	Write	vpc* (p. 714) aws:ResourceTag/ \${TagKey} (p. 717)	ec2:CreateTags route53:AssociateVPCWith HostedZone	ec2:ResourceTag/ \${TagKey} (p. 721) ec2:VpcID (p. 722)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-endpoint* (p. 713) aws:RequestTag/ \${TagKey} (p. 717)	aws:TagKeys (p. 717) ec2:VpceServiceName (p. 722) ec2:VpceServiceOwner (p. 722)	
			route-table (p. 705) aws:ResourceTag/ \${TagKey} (p. 717)	ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RouteTableID (p. 721)	
			security-group (p. 705) aws:ResourceTag/ \${TagKey} (p. 717)	ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SecurityGroupID (p. 721)	
			subnet (p. 705) aws:ResourceTag/ \${TagKey} (p. 717)	ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SubnetID (p. 722)	
					ec2:Region (p. 720)
CreateVpcEndpointConnectionNotification	Grants permission to create a connection notification for a VPC endpoint or VPC endpoint service	Write	vpc-endpoint (p. 713) aws:ResourceTag/ \${TagKey} (p. 717)	ec2:ResourceTag/ \${TagKey} (p. 721)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:Region (p. 720)
CreateVpcEndpointService	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* (p. 713) aws:RequestTag/ \${TagKey} (p. 717)	aws:TagKeys (p. 717) ec2:VpceServicePrivateDnsName (p. 722)	aws:RequestTag/ \${TagKey} (p. 717) ec2:Region (p. 720)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

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* (p. 714)	aws:ResourceTag/\${TagKey} (p. 717)	ec2:CreateTags
			vpc-peering-connection* (p. 714)	aws:RequestTag/\${TagKey} (p. 717) aws:TagKeys (p. 717)	ec2:AccepterVpc (p. 717) ec2:RequesterVpc (p. 721) ec2:VpcPeeringConnectionID (p. 722)
					ec2:Region (p. 720)
CreateVpnConnection	Grants permission to create a VPN connection between a virtual private gateway or transit gateway and a customer gateway	Write	customer-gateway* (p. 714)	aws:ResourceTag/\${TagKey} (p. 717)	ec2:CreateTags
					ec2:ResourceTag/\${TagKey} (p. 721)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions	
			vpn-connection*	aws:RequestTag/\${TagKey} (p. 718) aws:TagKeys (p. 717) ec2:AuthenticationType (p. 717) ec2:DPDTIMEoutSeconds (p. 718) ec2:GatewayType (p. 718) ec2:IKEVersions (p. 718) ec2:InsideTunnelCidr (p. 718) ec2:InsideTunnelIpv6Cidr (p. 718) ec2:Phase1DHGroup (p. 720) ec2:Phase1EncryptionAlgorithms (p. 720) ec2:Phase1IntegrityAlgorithms (p. 720) ec2:Phase1LifetimeSeconds (p. 720) ec2:Phase2DHGroup (p. 720) ec2:Phase2EncryptionAlgorithms (p. 720) ec2:Phase2IntegrityAlgorithms (p. 720) ec2:Phase2LifetimeSeconds (p. 720) ec2:PreSharedKeys (p. 720) ec2:RekeyFuzzPercentage (p. 721) ec2:RekeyMarginTimeSeconds (p. 721) ec2:ReplayWindowSizePackets (p. 721) ec2:RoutingType (p. 721)		
			transit-gateway	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)		
			vpn-gateway	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)		
					ec2:Region (p. 720)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateVpnConnectionRoute	Grants permission to create a static route for a VPN connection between a virtual private gateway and a customer gateway	Write	vpn-connection*	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	aws:RequestTag/CreateTags aws:TagKeys (p. 717) ec2:Region (p. 720)
CreateVpnGateway	Grants permission to create a virtual private gateway	Write	vpn-gateway*	aws:RequestTag/CreateTags aws:TagKeys (p. 717)	ec2:Region (p. 720)
DeleteCarrierGateway	Grants permission to delete a carrier gateway	Write	carrier-gateway*	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	aws:RequestTag/DeleteTags ec2:Region (p. 720)
DeleteClientVpnEndpoint	Grants permission to delete a Client VPN endpoint	Write	client-vpn-endpoint*	aws:ResourceTag/\${TagKey} (p. 717) ec2:ClientRootCertificateChainArn (p. 718) ec2:CloudwatchLogGroupArn (p. 718) ec2:CloudwatchLogStreamArn (p. 718) ec2:DirectoryArn (p. 718) ec2:ResourceTag/\${TagKey} (p. 721) ec2:SamlProviderArn (p. 721) ec2:ServerCertificateArn (p. 721)	aws:RequestTag/DeleteTags ec2:Region (p. 720)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

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* (p. 697) subnet (p. 708)	aws:ResourceTag/ {\$TagKey} (p. 717) ec2:ClientRootCertificateChainArn (p. 718) ec2:CloudwatchLogGroupArn (p. 718) ec2:CloudwatchLogStreamArn (p. 718) ec2:DirectoryArn (p. 718) ec2:ResourceTag/ {\$TagKey} (p. 721) ec2:SamlProviderArn (p. 721) ec2:ServerCertificateArn (p. 721)	
DeleteCoipPoolPermission	Grants permission to deny a service from accessing a customer owned IP (CoIP) pool [permission only]	Write			ec2:Region (p. 720)
DeleteCustomerGateway	Grants permission to delete a customer gateway	Write	customer-gateway* (p. 690)	aws:ResourceTag/ {\$TagKey} (p. 717) ec2:ResourceTag/ {\$TagKey} (p. 721)	ec2:Region (p. 720)
DeleteDhcpOption	Grants permission to delete a set of DHCP options	Write	dhcp-options* (p. 691)	aws:ResourceTag/ {\$TagKey} (p. 717) ec2:DhcpOptionsID (p. 718) ec2:ResourceTag/ {\$TagKey} (p. 721)	ec2:Region (p. 720)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteEgressOnlyInternetGateways	Grants permission to delete an egress-only internet gateway	Write	egress-only-internet-gateway* (p. 692) aws:ResourceTag/\${TagKey} (p. 717)	aws:ResourceTag/\${TagKey} (p. 721)	aws:ResourceTag/\${TagKey} (p. 717) ec2:Region (p. 720)
DeleteFleets	Grants permission to delete one or more EC2 Fleets	Write	fleet* (p. 692) aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	aws:ResourceTag/\${TagKey} (p. 717)	aws:ResourceTag/\${TagKey} (p. 717) ec2:Region (p. 720)
DeleteFlowLogs	Grants permission to delete one or more flow logs	Write	vpc-flow-log* (p. 713) aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	aws:ResourceTag/\${TagKey} (p. 717)	aws:ResourceTag/\${TagKey} (p. 717) ec2:Region (p. 720)
DeleteFpgaImage	Grants permission to delete an Amazon FPGA Image (AFI)	Write	fpga-image* (p. 695) aws:ResourceTag/\${TagKey} (p. 717) ec2:Owner (p. 719) ec2:Public (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)	aws:ResourceTag/\${TagKey} (p. 717)	aws:ResourceTag/\${TagKey} (p. 717) ec2:Region (p. 720)
DeleteInstanceEventWindows	Grants permission to delete the specified event window	Write	instance-event-window* (p. 695) aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	aws:ResourceTag/\${TagKey} (p. 717)	aws:ResourceTag/\${TagKey} (p. 717) ec2:Region (p. 720)
DeleteInternetGateways	Grants permission to delete an internet gateway	Write	internet-gateway* (p. 697) aws:ResourceTag/\${TagKey} (p. 717) ec2:InternetGatewayID (p. 719) ec2:ResourceTag/\${TagKey} (p. 721)	aws:ResourceTag/\${TagKey} (p. 717)	aws:ResourceTag/\${TagKey} (p. 717) ec2:Region (p. 720)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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* (p. 697)	ec2:ResourceTag/\${TagKey} (p. 721)	
					ec2:Region (p. 720)
DeleteIpamPool	Grants permission to delete an Amazon VPC IP Address Manager (IPAM) pool	Write	ipam-pool* (p. 697)	ec2:ResourceTag/\${TagKey} (p. 721)	
					ec2:Region (p. 720)
DeleteIpamScope	Grants permission to delete the scope for an Amazon VPC IP Address Manager (IPAM)	Write	ipam-scope* (p. 698)	ec2:ResourceTag/\${TagKey} (p. 721)	
					ec2:Region (p. 720)
DeleteKeyPair	Grants permission to delete a key pair by removing the public key from Amazon EC2	Write	key-pair (p. 699)	aws:ResourceTag/\${TagKey} (p. 717)	
				ec2:KeyPairName (p. 719)	ec2:KeyPairType (p. 719)
				ec2:ResourceTag/\${TagKey} (p. 721)	ec2:Region (p. 720)
DeleteLaunchTemplate	Grants permission to delete a launch template and its associated versions	Write	launch-template* (p. 699)	aws:ResourceTag/\${TagKey} (p. 717)	
				ec2:ResourceTag/\${TagKey} (p. 721)	ec2:Region (p. 720)
DeleteLaunchTemplateVersion	Grants permission to delete one or more versions of a launch template	Write	launch-template* (p. 699)	aws:ResourceTag/\${TagKey} (p. 717)	
				ec2:ResourceTag/\${TagKey} (p. 721)	ec2:Region (p. 720)
DeleteLocalGatewayRouteTable	Grants permission to delete a route from a local gateway route table	Write	local-gateway-route-table* (p. 700)	aws:ResourceTag/\${TagKey} (p. 717)	
				ec2:ResourceTag/\${TagKey} (p. 721)	ec2:Region (p. 720)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteLocalGatewayRoute [permission only]	Grants permission to deny a service from accessing a local gateway route table	Write	local-gateway-route-table* (p. 700)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
					ec2:Region (p. 720)
DeleteLocalGatewayRouteAssociation	Grants permission to delete an association between a VPC and local gateway route table	Write	local-gateway-route-table-vpc-association* (p. 700)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
					ec2:Region (p. 720)
DeleteManagedPrefixList	Grants permission to delete a managed prefix list	Write	prefix-list* (p. 704)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
					ec2:Region (p. 720)
DeleteNatGateway	Grants permission to delete a NAT gateway	Write	natgateway* (p. 704)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
					ec2:Region (p. 720)
DeleteNetworkAcl	Grants permission to delete a network ACL	Write	network-acl* (p. 701)	aws:ResourceTag/\${TagKey} (p. 717) ec2:NetworkAclID (p. 719) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Vpc (p. 722)	
					ec2:Region (p. 720)
DeleteNetworkAclEntry	Grants permission to delete an inbound or outbound entry (rule) from a network ACL	Write	network-acl* (p. 701)	aws:ResourceTag/\${TagKey} (p. 717) ec2:NetworkAclID (p. 719) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Vpc (p. 722)	
					ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteNetworkInsightsNetworkAccessScope	Grants permission to delete a Network Access Scope	Write	network-insights-access-scope* (p. 702)	ec2:ResourceTag/\${TagKey} (p. 721)	
				ec2:Region (p. 720)	
DeleteNetworkInsightsNetworkAccessScopeAnalysis	Grants permission to delete a Network Access Scope analysis	Write	network-insights-access-scope-analysis* (p. 702)	ec2:ResourceTag/\${TagKey} (p. 721)	
				ec2:Region (p. 720)	
DeleteNetworkInsightsNetworkInsightsAnalysis	Grants permission to delete a network insights analysis	Write	network-insights-analysis* (p. 702)	aws:ResourceTag/\${TagKey} (p. 717)	
				ec2:ResourceTag/\${TagKey} (p. 721)	ec2:Region (p. 720)
DeleteNetworkInsightsNetworkInsightsPath	Grants permission to delete a network insights path	Write	network-insights-path* (p. 702)	aws:ResourceTag/\${TagKey} (p. 717)	
				ec2:ResourceTag/\${TagKey} (p. 721)	ec2:Region (p. 720)
DeleteNetworkInterface	Grants permission to delete a detached network interface	Write	network-interface* (p. 702)	aws:ResourceTag/\${TagKey} (p. 717)	
				ec2:AvailabilityZone (p. 718) ec2:NetworkInterfaceID (p. 719) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Subnet (p. 721) ec2:Vpc (p. 722)	ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteNetworkInterfacePermission [permission that is]	Grants permission to delete a network interface that is associated with a network interface	Permissions management	network-interface (p. 703)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:AssociatePublicIpAddress (p. 717) ec2:AuthorizedService (p. 717) ec2:AvailabilityZone (p. 718) ec2:NetworkInterfaceID (p. 719) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:Subnet (p. 721) ec2:Vpc (p. 722)
					ec2:Region (p. 720)
DeletePlacementGroup	Grants permission to delete a placement group	Write	placement-group (p. 703)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:PlacementGroupName (p. 720) ec2:PlacementGroupStrategy (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721)
					ec2:Region (p. 720)
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* (p. 698)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:ResourceTag/ \${TagKey} (p. 721)
					ec2:Region (p. 720)
DeleteQueuedReservedInstancesPurchase	Grants permission to delete the queued purchases for the specified Reserved Instances	Write			ec2:Region (p. 720)
DeleteResourcePolicy [permission only]	Grants permission to remove an IAM policy that enables cross-account sharing from a resource	Write	ipam-pool (p. 697)	aws:ResourceTag/ \${TagKey} (p. 721)	ec2:ResourceTag/ \${TagKey} (p. 721)
					ec2:Region (p. 720)

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* (p. 705) prefix-list (p. 704)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RouteTableID (p. 721) ec2:Vpc (p. 722)	
DeleteRouteTable	Grants permission to delete a route table	Write	route-table* (p. 705)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RouteTableID (p. 721) ec2:Vpc (p. 722)	ec2:Region (p. 720)
DeleteSecurityGroup	Grants permission to delete a security group	Write	security-group* (p. 705)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SecurityGroupID (p. 721) ec2:Vpc (p. 722)	ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteSnapshot	Grants permission to delete a snapshot of an EBS volume	Write	snapshot* (p. 605) ResourceTag/ \${TagKey} (p. 717) ec2:OutpostArn (p. 719) ec2:Owner (p. 719) ec2:ParentVolume (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SnapshotID (p. 721) ec2:SnapshotTime (p. 721) ec2:SourceOutpostArn (p. 721) ec2:VolumeSize (p. 722)		ec2:Region (p. 720)
DeleteSpotDatafeedTopic	Grants permission to delete a data feed for Spot Instances	Write			ec2:Region (p. 720)
DeleteSubnet	Grants permission to delete a subnet	Write	subnet* (p. 709) aws:ResourceTag/ \${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SubnetID (p. 722) ec2:Vpc (p. 722)		ec2:Region (p. 720)
DeleteSubnetCidrBlock	Grants permission to delete a Subnet CIDR reservation	Write			ec2:Region (p. 720)
DeleteTags	Grants permission to delete one or more tags from Amazon EC2 resources	Tagging	capacity-reservation (p. 688) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		
	capacity-reservation-fleet (p. 688) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)				

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			client-vpn-endpoint (p. 691)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			customer-gateway (p. 690)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
		dedicated-host (p. 690)		aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
		dhcp-options (p. 690)		aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
		egress-only-internet-gateway (p. 691)		aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
		elastic-gpu (p. 691)		aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
		elastic-ip (p. 687)		aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
		export-image-task (p. 692)		aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
		export-instance-task (p. 692)		aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			fleet (p. 692) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		
			fpga- image (p. 693) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		
			host- reservation (p. 694) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		
			image (p. 694) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		
			import- image- task (p. 694) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		
			import- snapshot- task (p. 694) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		
			instance (p. 695) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		
			instance- event- window (p. 695) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		
			internet- gateway (p. 697) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		
	ipam (p. 697)		ec2:ResourceTag/ \${TagKey} (p. 721)		

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-pool (p. 697)	ec2:ResourceTag/\${TagKey} (p. 721)	
			ipam-scope (p. 698)	ec2:ResourceTag/\${TagKey} (p. 721)	
			ipv4pool-ec2 (p. 698)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			ipv6pool-ec2 (p. 698)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			key-pair (p. 699)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			launch-template (p. 700)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			local-gateway (p. 700)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			local-gateway-route-table (p. 700)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			local-gateway-route-table-virtual-interface-group-association (p. 700)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway-route-table-vpc-association (p. 702)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			local-gateway-virtual-interface (p. 702)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			local-gateway-virtual-interface-group (p. 701)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			natgateway (p. 702)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			network-acl (p. 701)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			network-insights-access-scope (p. 702)	ec2:ResourceTag/\${TagKey} (p. 721)	
			network-insights-access-scope-analysis (p. 702)	ec2:ResourceTag/\${TagKey} (p. 721)	
			network-interface (p. 703)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			placement-group (p. 703)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			prefix-list (p. 704) replace-root-volume-task (p. 704)	aws:ResourceTag/ {\$TagKey} (p. 717) ec2:ResourceTag/ {\$TagKey} (p. 721)	
			reserved-instances (p. 704)	aws:ResourceTag/ {\$TagKey} (p. 717) ec2:ResourceTag/ {\$TagKey} (p. 721)	
			route-table (p. 705) security-group (p. 705)	aws:ResourceTag/ {\$TagKey} (p. 717) ec2:ResourceTag/ {\$TagKey} (p. 721)	
			security-group-rule (p. 706)	aws:ResourceTag/ {\$TagKey} (p. 717) ec2:ResourceTag/ {\$TagKey} (p. 721)	
			snapshot (p. 707) spot-fleet-request (p. 708)	aws:ResourceTag/ {\$TagKey} (p. 717) ec2:ResourceTag/ {\$TagKey} (p. 721)	
			spot-instances-request (p. 708)	aws:ResourceTag/ {\$TagKey} (p. 717) ec2:ResourceTag/ {\$TagKey} (p. 721)	

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet (p. 708) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		
			subnet-cidr-reservation (p. 708) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		
			traffic-mirror-filter (p. 709) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		
			traffic-mirror-session (p. 710) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		
			traffic-mirror-target (p. 710) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		
			transit-gateway (p. 711) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		
			transit-gateway-attachment (p. 710) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		
			transit-gateway-connect-peer (p. 711) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		
			transit-gateway-multicast-domain (p. 711) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-route-table (p. 712)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			volume (p. 712)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			vpc (p. 714)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			vpc-endpoint (p. 713)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			vpc-endpoint-service (p. 713)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			vpc-flow-log (p. 713)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			vpc-peering-connection (p. 714)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			vpn-connection (p. 716)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			vpn-gateway (p. 717)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
				ec2:Region (p. 720)	

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTrafficMirrorFilter	Grants permission to delete a traffic mirror filter	Write	traffic-mirror-filter* (p. 709)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
					ec2:Region (p. 720)
DeleteTrafficMirrorFilterRule	Grants permission to delete a traffic mirror filter rule	Write	traffic-mirror-filter* (p. 709)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			traffic-mirror-filter-rule* (p. 709)		
					ec2:Region (p. 720)
DeleteTrafficMirrorSession	Grants permission to delete a traffic mirror session	Write	traffic-mirror-session* (p. 710)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
					ec2:Region (p. 720)
DeleteTrafficMirrorTarget	Grants permission to delete a traffic mirror target	Write	traffic-mirror-target* (p. 710)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
					ec2:Region (p. 720)
DeleteTransitGateway	Grants permission to delete a transit gateway	Write	transit-gateway* (p. 711)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
					ec2:Region (p. 720)
DeleteTransitGatewayConnectAttachment	Grants permission to delete a transit gateway connect attachment	Write	transit-gateway-attachment* (p. 710)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
					ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTransitGatewayConnectPeer	Grants permission to delete a transit gateway connect peer	Write	transit-gateway-connect-peer* (p. 711)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
					ec2:Region (p. 720)
DeleteTransitGatewayMulticastDomain	Grants permission to delete a transit gateway multicast domain	Write	transit-gateway-multicast-domain* (p. 712)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
					ec2:Region (p. 720)
DeleteTransitGatewayAttachment	Grants permission to delete a transit gateway attachment from a transit gateway	Write	transit-gateway-attachment* (p. 710)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
					ec2:Region (p. 720)
DeleteTransitGatewayPrefixListReference	Grants permission to delete a transit gateway prefix list reference	Write	prefix-list* (p. 704)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			transit-gateway-route-table* (p. 712)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
					ec2:Region (p. 720)
DeleteTransitGatewayRoute	Grants permission to delete a route from a transit gateway route table	Write	transit-gateway-route-table* (p. 712)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
					ec2:Region (p. 720)
DeleteTransitGatewayRouteTable	Grants permission to delete a transit gateway route table	Write	transit-gateway-route-table* (p. 712)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
					ec2:Region (p. 720)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTransitGatewayAttachment	Grants permission to delete a VPC attachment from a transit gateway	Write	transit-gateway-attachment*	aws:ResourceTag/\${TagKey} (p. 717) (p. 710) ec2:ResourceTag/\${TagKey} (p. 721)	
				ec2:Region (p. 720)	
DeleteVolume	Grants permission to delete an EBS volume	Write	volume* (p. 712) aws:ResourceTag/\${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:Encrypted (p. 718) ec2:ParentSnapshot (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:VolumeID (p. 722) ec2:VolumeIops (p. 722) ec2:VolumeSize (p. 722) ec2:VolumeThroughput (p. 722) ec2:VolumeType (p. 722)		
				ec2:Region (p. 720)	
DeleteVpc	Grants permission to delete a VPC	Write	vpc* (p. 714) aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Tenancy (p. 722) ec2:VpcID (p. 722)		
				ec2:Region (p. 720)	
DeleteVpcEndpoint <small>or DeleteVpcInterfaceEndpoint</small>	Grants permission to delete connection notifications	Write	vpc-endpoint (p. 713) aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)		
	vpc-endpoint-service (p. 713) aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)				
				ec2:Region (p. 720)	

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVpcEndpoint	Grants permission to delete one or more VPC endpoint service configurations	Write	vpc-endpoint-service* (p. 713)	aws:ResourceTag/\${TagKey} (p. 717)	
	ec2:ResourceTag/\${TagKey} (p. 721)			ec2:Region (p. 720)	
DeleteVpcEndpoints	Grants permission to delete one or more VPC endpoints	Write	vpc-endpoint* (p. 713)	aws:ResourceTag/\${TagKey} (p. 717)	
	ec2:ResourceTag/\${TagKey} (p. 721)			ec2:VpcServiceName (p. 722)	
DeleteVpcPeering	Grants permission to delete a VPC peering connection	Write	vpc-peering-connection* (p. 714)	aws:ResourceTag/\${TagKey} (p. 717)	ec2:AcceptorVpc (p. 717)
	ec2:RequesterVpc (p. 721)			ec2:ResourceTag/\${TagKey} (p. 721)	
DeleteVpnConnection	Grants permission to delete a VPN connection	Write	vpn-connection* (p. 713)	aws:ResourceTag/\${TagKey} (p. 717)	ec2:ResourceTag/\${TagKey} (p. 721)
	ec2:Region (p. 720)				
DeleteVpnConnections	Grants permission to delete a static route for a VPN connection between a virtual private gateway and a customer gateway	Write	vpn-connection* (p. 713)	aws:ResourceTag/\${TagKey} (p. 717)	ec2:ResourceTag/\${TagKey} (p. 721)
	ec2:Region (p. 720)				
DeleteVpnGateway	Grants permission to delete a virtual private gateway	Write	vpn-gateway* (p. 713)	aws:ResourceTag/\${TagKey} (p. 717)	ec2:ResourceTag/\${TagKey} (p. 721)
	ec2:Region (p. 720)				

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeprovisionByoipPool	Grants permission to release IP address range that was provisioned through bring your own IP addresses (BYOIP), and to delete the corresponding address pool	Write		ec2:Region (p. 720)	
DeprovisionIpamPool	Grants permission to deprovision IP address ranges provisioned from an Amazon VPC IP Address Manager (IPAM) pool	Write	ipam-pool* (p. 697)	ec2:ResourceTag/\${TagKey} (p. 721)	
					ec2:Region (p. 720)
DeprovisionPublicIpv4Pool	Grants permission to deprovision public IPv4 pools	Write	ipv4pool-ec2* (p. 698)	aws:ResourceTag/\${TagKey} (p. 717)	
				ec2:ResourceTag/\${TagKey} (p. 721)	
					ec2:Region (p. 720)
DeregisterImage	Grants permission to deregister an Amazon Machine Image (AMI)	Write	image* (p. 694) aws:ResourceTag/\${TagKey} (p. 717)	ec2:ImageID (p. 718) ec2:ImageType (p. 718) ec2:Owner (p. 719) ec2:Public (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RootDeviceType (p. 721)	
					ec2:Region (p. 720)
DeregisterInstancesTags	Grants permission to remove tags from the set of tags to include in notifications about scheduled events for your instances	Write		ec2:Region (p. 720)	

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeregisterTransitGatewayMulticastNetworkInterfaces	Grants permission to deregister One or more network interfaces members from a group IP address in a transit gateway multicast domain	Write	network-interface (p. 713)	aws:ResourceTag/\${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:NetworkInterfaceID (p. 719) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Subnet (p. 721) ec2:Vpc (p. 722)	
	transit-gateway-multicast-domain (p. 712)		aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)		
				ec2:Region (p. 720)	
DeregisterTransitGatewayMulticastNetworkSources	Grants permission to deregister One or more network interfaces sources from a group IP address in a transit gateway multicast domain	Write	network-interface (p. 713)	aws:ResourceTag/\${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:NetworkInterfaceID (p. 719) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Subnet (p. 721) ec2:Vpc (p. 722)	
	transit-gateway-multicast-domain (p. 712)		aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)		
				ec2:Region (p. 720)	
DescribeAccountAttributes	Grants permission to describe The attributes of the AWS account	List			ec2:Region (p. 720)
DescribeAddresses	Grants permission to describe One or more Elastic IP addresses	List			ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeAddresses	Grants permission to describe the attribute of the specified Elastic IP addresses	List	elastic-ip (p. 687)	aws:ResourceTag/ \${TagKey} (p. 717)	
	ec2:AllocationId (p. 717)			ec2:Domain (p. 718)	
DescribeAggregateFleets	Grants permission to describe the longer ID format settings for all resource types	List		ec2:PublicIpAddress (p. 720)	
	ec2:ResourceTag / \${TagKey} (p. 721)			ec2:Region (p. 720)	
DescribeAvailabilityZones	Grants permission to describe one or more of the Availability Zones that are available to you	List		ec2:Region (p. 720)	
DescribeBundleTasks	Grants permission to describe one or more bundling tasks	List		ec2:Region (p. 720)	
DescribeByoipCidrs	Grants permission to describe the IP address ranges that were provisioned through bring your own IP addresses (BYOIP)	List		ec2:Region (p. 720)	
DescribeCapacityReservations	Grants permission to describe one or more Capacity Reservation Fleets	List		ec2:Region (p. 720)	
DescribeCapacityReserveOfferings	Grants permission to describe one or more Capacity Reservations	List		ec2:Region (p. 720)	
DescribeCarrierGateways	Grants permission to describe one or more Carrier Gateways	List		ec2:Region (p. 720)	
DescribeClassicLinkInstances	Grants permission to describe one or more linked EC2-Classic instances	List		ec2:Region (p. 720)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeClientVpnAuthorizationRules	Grants permission to describe the authorization rules for a Client VPN endpoint	List	client-vpn-endpoint (p. 699)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ClientRootCertificateChainArn (p. 718) ec2:CloudwatchLogGroupArn (p. 718) ec2:CloudwatchLogStreamArn (p. 718) ec2:DirectoryArn (p. 718) ec2:ResourceTag/\${TagKey} (p. 721) ec2:SamlProviderArn (p. 721) ec2:ServerCertificateArn (p. 721)	ec2:Region (p. 720)
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 (p. 699)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ClientRootCertificateChainArn (p. 718) ec2:CloudwatchLogGroupArn (p. 718) ec2:CloudwatchLogStreamArn (p. 718) ec2:DirectoryArn (p. 718) ec2:ResourceTag/\${TagKey} (p. 721) ec2:SamlProviderArn (p. 721) ec2:ServerCertificateArn (p. 721)	ec2:Region (p. 720)
DescribeClientVpnEndpoints	Grants permission to describe one or more Client VPN endpoints	List	client-vpn-endpoint (p. 699)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ClientRootCertificateChainArn (p. 718) ec2:CloudwatchLogGroupArn (p. 718) ec2:CloudwatchLogStreamArn (p. 718) ec2:DirectoryArn (p. 718) ec2:ResourceTag/\${TagKey} (p. 721) ec2:SamlProviderArn (p. 721) ec2:ServerCertificateArn (p. 721)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:Region (p. 720)
DescribeClientVpnRoutes	Grants permission to describe the routes for a Client VPN endpoint	List	client-vpn-endpoint (p. 717)	aws:ResourceTag/ {\$TagKey} (p. 717) ec2:ClientRootCertificateChainArn (p. 718) ec2:CloudwatchLogGroupArn (p. 718) ec2:CloudwatchLogStreamArn (p. 718) ec2:DirectoryArn (p. 718) ec2:ResourceTag/ {\$TagKey} (p. 721) ec2:SamlProviderArn (p. 721) ec2:ServerCertificateArn (p. 721)	
					ec2:Region (p. 720)
DescribeClientVpnTargetNetworks	Grants permission to describe the target networks that are associated with a Client VPN endpoint	List	client-vpn-endpoint (p. 717)	aws:ResourceTag/ {\$TagKey} (p. 717) ec2:ClientRootCertificateChainArn (p. 718) ec2:CloudwatchLogGroupArn (p. 718) ec2:CloudwatchLogStreamArn (p. 718) ec2:DirectoryArn (p. 718) ec2:ResourceTag/ {\$TagKey} (p. 721) ec2:SamlProviderArn (p. 721) ec2:ServerCertificateArn (p. 721)	
					ec2:Region (p. 720)
DescribeCoiPPool	Grants permission to describe the specified customer-owned address pools or all of your customer-owned address pools	List			ec2:Region (p. 720)
DescribeConversionTasks	Grants permission to describe one or more conversion tasks	List			ec2:Region (p. 720)
DescribeCustomerGateways	Grants permission to describe one or more customer gateways	List			ec2:Region (p. 720)
DescribeDhcpOptions	Grants permission to describe one or more DHCP options sets	List			ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeEgressOnlyInternetGateways	Grants permission to describe one or more Egress Only Internet Gateways	List		ec2:Region (p. 720)	
DescribeElasticGpus	Grants permission to describe an Elastic Graphics accelerator that is associated with an instance	Read		ec2:Region (p. 720)	
DescribeExportImageTasks	Grants permission to describe one or more export image tasks	List		ec2:Region (p. 720)	
DescribeExportTasks	Grants permission to describe one or more export instance tasks	List		ec2:Region (p. 720)	
DescribeFastLaunchAMIs	Grants permission to describe fast-launch enabled Windows AMIs	Read	image (p. 694) aws:ResourceTag/\${TagKey} (p. 717)		
			ec2:ImageID (p. 718) ec2:ImageType (p. 718) ec2:Owner (p. 719) ec2:Public (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RootDeviceType (p. 721)	ec2:Region (p. 720)	
DescribeFastSnapshotRestores	Grants permission to describe the state of fast snapshot restores for snapshots	Read		ec2:Region (p. 720)	
DescribeFleetHistory	Grants permission to describe the events for an EC2 Fleet during a specified time	List	fleet (p. 692) aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)		
				ec2:Region (p. 720)	
DescribeFleetInstances	Grants permission to describe the running instances for an EC2 Fleet	List	fleet (p. 692) aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)		
				ec2:Region (p. 720)	

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeFleets	Grants permission to describe one or more EC2 Fleets	List	fleet (p. 692)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)	
	ec2:Region (p. 720)				
DescribeFlowLogs	Grants permission to describe one or more flow logs	List		ec2:Region (p. 720)	
DescribeFpgaImageAttribute	Grants permission to describe the attributes of an Amazon FPGA Image (AFI)	List	fpga-image* (p. 699)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:Attribute/ \${AttributeName} (p. 717) ec2:Owner (p. 719) ec2:Public (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721)	
ec2:Region (p. 720)					
DescribeFpgaImages	Grants permission to describe one or more Amazon FPGA Images (AFIs)	List		ec2:Region (p. 720)	
DescribeHostReservations	Grants permission to describe the Dedicated Host Reservations that are available to purchase	List		ec2:Region (p. 720)	
DescribeHostReservations	Grants permission to describe the Dedicated Host Reservations that are associated with Dedicated Hosts in the AWS account	List		ec2:Region (p. 720)	
DescribeHosts	Grants permission to describe one or more Dedicated Hosts	List		ec2:Region (p. 720)	
DescribeIamInstanceProfiles	Grants permission to describe the IAM instance profile associations	List		ec2:Region (p. 720)	
DescribeIdFormat	Grants permission to describe the ID format settings for resources	List		ec2:Region (p. 720)	
DescribeIdentityIdFormat	Grants permission to describe the ID format settings for resources for an IAM user, IAM role, or root user	List		ec2:Region (p. 720)	

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 (p. 694) aws:ResourceTag/ \${TagKey} (p. 717)	ec2:ImageID (p. 718) ec2:ImageType (p. 718) ec2:Owner (p. 719) ec2:Public (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721)	ec2:RootDeviceType (p. 721)
				ec2:Region (p. 720)	
DescribeImages	Grants permission to describe one or more images (AMIs, AKIs, and ARIs)	List			ec2:Region (p. 720)
DescribeImportImageTasks	Grants permission to describe import tasks virtual machine or import snapshot tasks	List			ec2:Region (p. 720)
DescribeImportSnapshotTasks	Grants permission to describe import snapshot tasks	List			ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeInstances <small>The attributes of an instance</small>	Grants permission to describe the attributes of an instance	List	instance (p. 696); ResourceTag/ \${TagKey} (p. 717)		ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceAutoRecovery (p. 719) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceMetadataTags (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:PlacementGroup (p. 720) ec2:ProductCode (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)
	ec2:Region (p. 720)				
DescribeInstances <small>The CPU burst option for CPU usage of one or more burstable performance instances</small>	Grants permission to describe the CPU burst option for CPU usage of one or more burstable performance instances	List			ec2:Region (p. 720)
DescribeInstances <small>The set of tags to include in notifications about scheduled events for your instances</small>	Grants permission to describe the set of tags to include in notifications about scheduled events for your instances	List			ec2:Region (p. 720)
DescribeInstances <small>The specified event windows or all event windows</small>	Grants permission to describe the specified event windows or all event windows	List			ec2:Region (p. 720)
DescribeInstances <small>The status of one or more instances</small>	Grants permission to describe the status of one or more instances	List			ec2:Region (p. 720)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeInstances	Grants permission to describe The set of instance types that are offered in a location	List		ec2:Region (p. 720)	
DescribeInstanceTypes	Grants permission to describe The details of instance types that are offered in a location	List		ec2:Region (p. 720)	
DescribeInstances	Grants permission to describe one or more instances	List		ec2:Region (p. 720)	
DescribeInternetGateways	Grants permission to describe one or more internet gateways	List		ec2:Region (p. 720)	
DescribeIpamPools	Grants permission to describe Amazon VPC IP Address Manager (IPAM) pools	List		ec2:Region (p. 720)	
DescribeIpamScopes	Grants permission to describe Amazon VPC IP Address Manager (IPAM) scopes	List		ec2:Region (p. 720)	
DescribeIpams	Grants permission to describe an Amazon VPC IP Address Manager (IPAM)	List		ec2:Region (p. 720)	
DescribeIpv6Pools	Grants permission to describe one or more IPv6 address pools	List		ec2:Region (p. 720)	
DescribeKeyPairs	Grants permission to describe one or more key pairs	List		ec2:Region (p. 720)	
DescribeLaunchTemplateVersions	Grants permission to describe one or more launch template versions	List		ec2:Region (p. 720)	
DescribeLaunchTemplates	Grants permission to describe one or more launch templates	List		ec2:Region (p. 720)	
DescribeLocalGateways [permission only]	Grants permission to allow a service to describe local gateway route table permissions	List		ec2:Region (p. 720)	
DescribeLocalGatewayVirtualInterfaceGroups	Grants permission to describe the associations between virtual interface groups and local gateway route tables	List		ec2:Region (p. 720)	
DescribeLocalGatewayVirtualInterfaceGroupAssociations	Grants permission to describe the associations between virtual interface groups and local gateway route tables	List		ec2:Region (p. 720)	
DescribeLocalGatewayRouteTables	Grants permission to describe one or more local gateway route tables	List		ec2:Region (p. 720)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeLocalGatewayVirtualInterfaceGroups	Grants permission to describe local gateway virtual interface groups	List		ec2:Region (p. 720)	
DescribeLocalGatewayVirtualInterfaces	Grants permission to describe local gateway virtual interfaces	List		ec2:Region (p. 720)	
DescribeLocalGateways	Grants permission to describe one or more local gateways	List		ec2:Region (p. 720)	
DescribeManagedPrefixLists	Grants permission to describe your managed prefix lists and any AWS-managed prefix lists	List		ec2:Region (p. 720)	
DescribeMovingAddresses	Grants permission to describe Elastic IP addresses that are being moved to the EC2-VPC platform	List		ec2:Region (p. 720)	
DescribeNatGateways	Grants permission to describe one or more NAT gateways	List		ec2:Region (p. 720)	
DescribeNetworkACLs	Grants permission to describe one or more network ACLs	List		ec2:Region (p. 720)	
DescribeNetworkAccessScopes	Grants permission to describe one or more Network Access Scope analyses	List		ec2:Region (p. 720)	
DescribeNetworkInsightsAnalyses	Grants permission to describe one or more network insights analyses	List		ec2:Region (p. 720)	
DescribeNetworkInsightsPaths	Grants permission to describe one or more network insights paths	List		ec2:Region (p. 720)	
DescribeNetworkInterfaceAttribute	Grants permission to describe a network interface attribute	List		ec2:Region (p. 720)	
DescribeNetworkInterfacePermissions	Grants permission to describe the permissions that are associated with a network interface	List		ec2:Region (p. 720)	
DescribeNetworkInterfaces	Grants permission to describe one or more network interfaces	List		ec2:Region (p. 720)	
DescribePlacementGroups	Grants permission to describe one or more placement groups	List		ec2:Region (p. 720)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribePrefixList	Grants permission to describe available AWS services in a prefix list format	List		ec2:Region (p. 720)	
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 (p. 720)	
DescribePublicIpv4AddressPools	Grants permission to describe one or more IPv4 address pools	List		ec2:Region (p. 720)	
DescribeRegions	Grants permission to describe one or more AWS Regions that are currently available in your account	List		ec2:Region (p. 720)	
DescribeReplaceRootVolumeTask	Grants permission to describe a Root volume replacement task	List		ec2:Region (p. 720)	
DescribeReservedInstances	Grants permission to describe one or more purchased Reserved Instances in your account	List		ec2:Region (p. 720)	
DescribeReservedInstancesListings	Grants permission to describe your marketplace Reserved Instance listings in the Reserved Instance Marketplace	List		ec2:Region (p. 720)	
DescribeReservedInstancesOfferings	Grants permission to describe the modifications trade to one or more Reserved Instances	List		ec2:Region (p. 720)	
DescribeRouteTables	Grants permission to describe one or more route tables	List		ec2:Region (p. 720)	
DescribeScheduledInstances	Grants permission to find available schedules for Scheduled Instances	Read		ec2:Region (p. 720)	
DescribeScheduledInstances	Grants permission to describe one or more Scheduled Instances in your account	Read		ec2:Region (p. 720)	
DescribeSecurityGroups	Grants permission to describe the VPCs on the other side of a VPC peering connection that are referencing specified VPC security groups	List		ec2:Region (p. 720)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeSecurityGroups	Grants permission to describe one or more security group rules	List		ec2:Region (p. 720)	
DescribeSecurityGroups	Grants permission to describe one or more security groups	List		ec2:Region (p. 720)	
DescribeSnapshotAttribute	Grants permission to describe an attribute of a snapshot	List	snapshot (p. 707) ResourceTag/ \${TagKey} (p. 717)	ec2:AvailabilityZone (p. 718) ec2:Encrypted (p. 718) ec2:OutpostArn (p. 719) ec2:Owner (p. 719) ec2:ParentVolume (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SnapshotID (p. 721) ec2:SnapshotTime (p. 721) ec2:SourceOutpostArn (p. 721) ec2:VolumeSize (p. 722)	ec2:Region (p. 720)
DescribeSnapshotStorageTierStatus	Grants permission to describe the storage tier status for Amazon EBS snapshots	List		ec2:Region (p. 720)	
DescribeSnapshots	Grants permission to describe one or more EBS snapshots	List		ec2:Region (p. 720)	
DescribeSpotDatafeedSubscription	Grants permission to describe the data feed for Spot Instances	List		ec2:Region (p. 720)	
DescribeSpotFleetRunningInstances	Grants permission to describe the running instances for a Spot Fleet	List	spot-fleet-request (p. 708) ResourceTag/ \${TagKey} (p. 717)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)	ec2:Region (p. 720)
DescribeSpotFleetEvents	Grants permission to describe the events for a Spot Fleet request during a specified time	List	spot-fleet-request (p. 708) ResourceTag/ \${TagKey} (p. 717)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)	

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:Region (p. 720)
DescribeSpotFleetRequestOptions	Grants permission to describe one or more Spot Fleet requests	List			ec2:Region (p. 720)
DescribeSpotInstanceHistory	Grants permission to describe one or more Spot Instance requests	List			ec2:Region (p. 720)
DescribeSpotPriceHistory	Grants permission to describe the Spot Instance price history	List			ec2:Region (p. 720)
DescribeStaleSecurityGroupRules	Grants permission to describe the stale security group rules for security groups in a specified VPC	List			ec2:Region (p. 720)
DescribeStoreImageTasks	Grants permission to describe the progress of the AMI store tasks	List	image (p. 694) aws:ResourceTag/\${TagKey} (p. 717) ec2:ImageID (p. 718) ec2:ImageType (p. 718) ec2:Owner (p. 719) ec2:Public (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RootDeviceType (p. 721)		ec2:Region (p. 720)
DescribeSubnets	Grants permission to describe one or more subnets	List			ec2:Region (p. 720)
DescribeTags	Grants permission to describe one or more tags for an Amazon EC2 resource	Read			ec2:Region (p. 720)
DescribeTrafficMirrorFilters	Grants permission to describe one or more traffic mirror filters	List			ec2:Region (p. 720)
DescribeTrafficMirrorSessions	Grants permission to describe one or more traffic mirror sessions	List			ec2:Region (p. 720)
DescribeTrafficMirrorTargets	Grants permission to describe one or more traffic mirror targets	List			ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeTransitGatewayAttachments	Grants permission to describe one or more transit gateway attachments between resources and transit gateways	List		ec2:Region (p. 720)	
DescribeTransitGatewayConnectPeers	Grants permission to describe one or more transit gateway connect peers	List		ec2:Region (p. 720)	
DescribeTransitGatewayConnectAttachments	Grants permission to describe one or more transit gateway connect attachments	List		ec2:Region (p. 720)	
DescribeTransitGatewayMulticastDominos	Grants permission to describe one or more transit gateway multicast domains	List		ec2:Region (p. 720)	
DescribeTransitGatewayPeerAttachments	Grants permission to describe one or more transit gateway peering attachments	List		ec2:Region (p. 720)	
DescribeTransitGatewayRouteTables	Grants permission to describe one or more transit gateway route tables	List		ec2:Region (p. 720)	
DescribeTransitGatewayVpcAttachments	Grants permission to describe one or more VPC attachments on a transit gateway	List		ec2:Region (p. 720)	
DescribeTransitGateways	Grants permission to describe one or more transit gateways	List		ec2:Region (p. 720)	
DescribeTrunkInterfaceAssociations	Grants permission to describe one or more network interface trunk associations	List		ec2:Region (p. 720)	

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeVolumeAttribute	Grants permission to describe an attribute of an EBS volume	List	volume (p. 712) aws:ResourceTag/ \${TagKey} (p. 717)	ec2:AvailabilityZone (p. 718) ec2:Encrypted (p. 718) ec2:KmsKeyId (p. 719) ec2:ParentSnapshot (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:VolumeID (p. 722) ec2:VolumeIops (p. 722) ec2:VolumeSize (p. 722) ec2:VolumeThroughput (p. 722) ec2:VolumeType (p. 722)	ec2:Region (p. 720)
DescribeVolumeStatus	Grants permission to describe the status of one or more EBS volumes	List		ec2:Region (p. 720)	
DescribeVolumes	Grants permission to describe one or more EBS volumes	List		ec2:Region (p. 720)	
DescribeVolumeModification	Grants permission to describe the modification status of one or more EBS volumes	Read		ec2:Region (p. 720)	
DescribeVpcAttribute	Grants permission to describe an attribute of a VPC	List	vpc* (p. 714) aws:ResourceTag/ \${TagKey} (p. 717)	ec2:ResourceTag/ \${TagKey} (p. 721) ec2:Tenancy (p. 722) ec2:VpcID (p. 722)	ec2:Region (p. 720)
DescribeVpcClassicLink	Grants permission to describe the ClassicLink status of one or more VPCs	List		ec2:Region (p. 720)	
DescribeVpcClassicLinkDnsSupport	Grants permission to describe the ClassicLink DNS support status of one or more VPCs	List		ec2:Region (p. 720)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeVpcEndpointConnectionNotifications	Grants permission to describe VPC endpoint connections to your VPC endpoint services	List		ec2:Region (p. 720)	
DescribeVpcEndpointConnections	Grants permission to describe VPC endpoint connections to your VPC endpoint services	List		ec2:Region (p. 720)	
DescribeVpcEndpointServiceConfigurations	Grants permission to describe VPC endpoint service configurations (your services)	List		ec2:Region (p. 720)	
DescribeVpcEndpointServices	Grants permission to describe the principal services consumers) that are permitted to discover your VPC endpoint service	List		ec2:Region (p. 720)	
DescribeVpcEndpoints	Grants permission to describe all supported AWS services that can be specified when creating a VPC endpoint	List		ec2:Region (p. 720)	
DescribeVpcEndpoints	Grants permission to describe one or more VPC endpoints	List		ec2:Region (p. 720)	
DescribeVpcPeeringConnections	Grants permission to describe one or more VPC peering connections	List		ec2:Region (p. 720)	
DescribeVpcs	Grants permission to describe one or more VPCs	List		ec2:Region (p. 720)	
DescribeVpnConnections	Grants permission to describe one or more VPN connections	Read		ec2:Region (p. 720)	
DescribeVpnGateways	Grants permission to describe one or more virtual private gateways	List		ec2:Region (p. 720)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DetachClassicLink (Detach)	Grants permission to unlink (Detach) a linked EC2-Classic instance from a VPC	Write	instance* (p. 695) aws:ResourceTag/ \${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceID (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLim ec2:MetadataHttpTokens (p. 719) ec2:PlacementGroup (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)		
	vpc* (p. 714)		aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:Tenancy (p. 722) ec2:VpcID (p. 722)		
			ec2:Region (p. 720)		
DetachInternetGateway	Grants permission to detach an internet gateway from a VPC	Write	internet-gateway* (p. 697) aws:ResourceTag/ \${TagKey} (p. 717) ec2:InternetGatewayID (p. 719) ec2:ResourceTag/ \${TagKey} (p. 721)		

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc* (p. 714)	aws:ResourceTag/ \${TagKey} (p. 717)	
			ec2:ResourceTag/ \${TagKey} (p. 721)	ec2:Tenancy (p. 722)	
			ec2:VpcID (p. 722)		ec2:Region (p. 720)
DetachNetworkInterface	Grants permission to detach network interface from an instance	Write	instance* (p. 696)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceAutoRecovery (p. 719) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceMetadataTags (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:PlacementGroup (p. 720) ec2:ProductCode (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-interface* (p. 703)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:AvailabilityZone (p. 718) ec2:NetworkInterfaceID (p. 719) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:Subnet (p. 721) ec2:Vpc (p. 722)
DetachVolume	Grants permission to detach an EBS volume from an instance	Write	volume* (p. 703)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:AvailabilityZone (p. 718) ec2:Encrypted (p. 718) ec2:ParentSnapshot (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:VolumeID (p. 722) ec2:VolumeIops (p. 722) ec2:VolumeSize (p. 722) ec2:VolumeThroughput (p. 722) ec2:VolumeType (p. 722)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance (p. 696);ResourceTag/\${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:PlacementGroup (p. 720) ec2:ProductCode (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)		ec2:Region (p. 720)
DetachVpnGateway	Grants permission to detach a virtual private gateway from a VPC	Write	vpc* (p. 714)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Tenancy (p. 722) ec2:VpcID (p. 722)	
			vpn-gateway* (p. 717)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
					ec2:Region (p. 720)
DisableEbsEncryptionOptionally	Grants permission to disable EBS encryption by default for your account	Write			ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableFastLaunch	Grants permission to disable faster launching for Windows AMIs	Write	image (p. 694) aws:ResourceTag/\${TagKey} (p. 717) ec2:ImageID (p. 718) ec2:ImageType (p. 718) ec2:Owner (p. 719) ec2:Public (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RootDeviceType (p. 721)		
			ec2:Region (p. 720)		
DisableFastSnapshotRestore	Grants permission to disable fast snapshot restores for one or more snapshots in specified Availability Zones	Write	snapshot* (p. 697) aws:ResourceTag/\${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:Encrypted (p. 718) ec2:Owner (p. 719) ec2:ParentVolume (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:SnapshotID (p. 721) ec2:SnapshotTime (p. 721) ec2:VolumeSize (p. 722)		
			ec2:Region (p. 720)		
DisableImageDeprecation	Grants permission to cancel the deprecation of the specified AMI	Write	image* (p. 694) aws:ResourceTag/\${TagKey} (p. 717) ec2:ImageID (p. 718) ec2:ImageType (p. 718) ec2:Owner (p. 719) ec2:Public (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RootDeviceType (p. 721)		
			ec2:Region (p. 720)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableIpamOrganizationMember	Grants permission to disable an AWS Organizations member account as an Amazon VPC IP Address Manager (IPAM) admin account	Write		ec2:Region (p. 720)	organizations:DeregisterMember
DisableSerialConsoleAccess	Grants permission to disable access to the EC2 serial console of all instances for your account	Write		ec2:Region (p. 720)	
DisableTransitGatewayAttachmentPropagation	Grants permission to disable a resource attachment from propagating routes to the specified propagation route table	Write	transit-gateway-attachment*	aws:ResourceTag/\${TagKey} (p. 717)	(p. 710)
			transit-gateway-route-table*	aws:ResourceTag/\${TagKey} (p. 717)	ec2:ResourceTag/\${TagKey} (p. 721)
					ec2:Region (p. 720)
DisableVgwRoutePropagation	Grants permission to disable a virtual private gateway from propagating routes to a specified route table of a VPC	Write	route-table* (p. 705)	aws:ResourceTag/\${TagKey} (p. 717)	
				ec2:ResourceTag/\${TagKey} (p. 721)	ec2:RouteTableID (p. 721)
				ec2:Vpc (p. 722)	
DisableVpcClassicLink	Grants permission to disable ClassicLink for a VPC	Write	vpn-gateway* (p. 714)	aws:ResourceTag/\${TagKey} (p. 717)	
				ec2:ResourceTag/\${TagKey} (p. 721)	ec2:Tenancy (p. 722)
		ec2:VpcID (p. 722)			ec2:Region (p. 720)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableVpcClassicLinkDNS	Grants permission to disable ClassicLink DNS support for a VPC	Write	vpc (p. 714)	aws:ResourceTag/ {\$TagKey} (p. 717)	
	ec2:ResourceTag/ {\$TagKey} (p. 721) ec2:Tenancy (p. 722) ec2:VpcID (p. 722)			ec2:Region (p. 720)	
DisassociateAddress	Grants permission to disassociate an Elastic IP address from an instance or network interface	Write	elastic-ip (p. 687)	aws:ResourceTag/ {\$TagKey} (p. 717) ec2:AllocationId (p. 717) ec2:Domain (p. 718) ec2:PublicIpAddress (p. 720) ec2:ResourceTag/ {\$TagKey} (p. 721)	
	aws:ResourceTag/ {\$TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:NetworkInterfaceID (p. 719) ec2:ResourceTag/ {\$TagKey} (p. 721) ec2:Subnet (p. 721) ec2:Vpc (p. 722)			ec2:Region (p. 720)	
DisassociateClientEndpointTargetNetwork	Grants permission to disassociate target network from a Client VPN endpoint	Write	client-vpn-endpoint* (p. 719)	aws:ResourceTag/ {\$TagKey} (p. 717) ec2:ClientRootCertificateChainArn (p. 718) ec2:CloudwatchLogGroupArn (p. 718) ec2:CloudwatchLogStreamArn (p. 718) ec2:DirectoryArn (p. 718) ec2:ResourceTag/ {\$TagKey} (p. 721) ec2:SamlProviderArn (p. 721) ec2:ServerCertificateArn (p. 721)	

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region (p. 720)	
DisassociateEnclaveCertificateFromRole	Grants permission to disassociate an ACM certificate from a IAM role	Write	certificate* (p. 689)		
			role* (p. 705)		
				ec2:Region (p. 720)	
DisassociateInstanceProfile	Grants permission to disassociate an IAM instance profile from a running or stopped instance	Write	instance* (p. 696)	ResourceTag/\${TagKey} (p. 717)	
				ec2:AvailabilityZone (p. 718)	
				ec2:EbsOptimized (p. 718)	
				ec2:InstanceAutoRecovery (p. 719)	
				ec2:InstanceId (p. 719)	
				ec2:InstanceMarketType (p. 719)	
				ec2:InstanceMetadataTags (p. 719)	
				ec2:InstanceProfile (p. 719)	
				ec2:InstanceType (p. 719)	
				ec2:MetadataHttpEndpoint (p. 719)	
DisassociateInstancesFromEventWindow	Grants permission to disassociate one or more targets from an event window	Write	ec2:MetadataHttpPutResponseHopLimit		
				ec2:MetadataHttpTokens (p. 719)	
				ec2:PlacementGroup (p. 720)	
DisassociateProductCodeFromInstance	Grants permission to disassociate a product code from an instance	Write	ec2:ProductCode (p. 720)		
				ec2:ResourceTag/\${TagKey} (p. 721)	
				ec2:RootDeviceType (p. 721)	
DisassociateRootVolumeFromInstance	Grants permission to disassociate a root volume from an instance	Write	ec2:Tenancy (p. 722)		
					ec2:Region (p. 720)
DisassociateTargetsFromEventWindow	Grants permission to disassociate one or more targets from an event window	Write	aws:ResourceTag/\${TagKey} (p. 717)		
				695	
				ec2:ResourceTag/\${TagKey} (p. 721)	
DisassociateVolumeFromInstance	Grants permission to disassociate a volume from an instance	Write		ec2:Region (p. 720)	

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateRouteTable	Grants permission to disassociate a subnet from a route table	Write	route-table (p. 705) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RouteTableID (p. 721) ec2:Vpc (p. 722)		
	subnet (p. 709) aws:ResourceTag/ \${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SubnetID (p. 722) ec2:Vpc (p. 722)				
	ec2:Region (p. 720)				
DisassociateSubnetCidrBlock	Grants permission to disassociate a CIDR block from a subnet	Write	subnet* (p. 709) aws:ResourceTag/ \${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SubnetID (p. 722) ec2:Vpc (p. 722)		
	ec2:Region (p. 720)				
DisassociateTransitGatewayAttachment	Grants permission to disassociate one or more subnets from a transit gateway multicast domain	Write	subnet* (p. 709) aws:ResourceTag/ \${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SubnetID (p. 722) ec2:Vpc (p. 722)		
	transit-gateway-attachment* aws:ResourceTag/ \${TagKey} (p. 710) ec2:ResourceTag/ \${TagKey} (p. 721)				

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-multicast-domain* (p. 710)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
DisassociateTransitGatewayRouteTable	Grants permission to disassociate a route table attachment from a transit gateway route table	Write	transit-gateway-attachment*	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			transit-gateway-route-table* (p. 712)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
				ec2:Region (p. 720)	
DisassociateTrunkInterface	Grants permission to disassociate a branch network interface to a trunk network interface	Write			ec2:Region (p. 720)
DisassociateVpcCidrBlock	Grants permission to disassociate a CIDR block from a VPC	Write	vpc (p. 714)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Tenancy (p. 722) ec2:VpcID (p. 722)	
				ec2:Region (p. 720)	
EnableEbsEncryptionByDefault	Grants permission to enable EBS encryption by default for your account	Write			ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableFastLaunch	Grants permission to enable faster launching for Windows AMIs	Write	image (p. 694) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ImageID (p. 718) ec2:ImageType (p. 718) ec2:Owner (p. 719) ec2:Public (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RootDeviceType (p. 721)		
	launch- template (p. 694) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)				
				ec2:Region (p. 720)	
EnableFastSnapshot	Grants permission to enable fast snapshot restores for one or more snapshots in specified Availability Zones	Write	snapshot* (p. 707) aws:ResourceTag/ \${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:Encrypted (p. 718) ec2:Owner (p. 719) ec2:ParentVolume (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SnapshotID (p. 721) ec2:SnapshotTime (p. 721) ec2:VolumeSize (p. 722)		
				ec2:Region (p. 720)	

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* (p. 694) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ImageID (p. 718) ec2:ImageType (p. 718) ec2:Owner (p. 719) ec2:Public (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RootDeviceType (p. 721)		
			ec2:Region (p. 720)		
EnableIpamOrganizationAccess	Grants permission to enable an AWS Organizations member account as an Amazon VPC IP Address Manager (IPAM) admin account	Write		ec2:Region (p. 720) CreateServiceLinkedRole (p. 720) organizations:EnableAWSOrganizationsFeature (p. 720) organizations:RegisterDefaultIpamScope (p. 720)	
EnableSerialConsoleAccess	Grants permission to enable access to the EC2 serial console of all instances for your account	Write		ec2:Region (p. 720)	
EnableTransitGatewayAttachmentToPropagationRouteTable	Grants permission to enable an attachment to propagation routes to a propagation route table	Write	transit-gateway-attachment* (p. 710)	aws:ResourceTag/ \${TagKey} (p. 717) (p. 710) ec2:ResourceTag/ \${TagKey} (p. 721)	
	transit-gateway-route-table* (p. 712)		aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		
			ec2:Region (p. 720)		
EnableVgwRoutePropagation	Grants permission to enable a virtual private gateway to propagate routes to a VPC route table	Write	route-table* (p. 705)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RouteTableID (p. 721) ec2:Vpc (p. 722)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpn-gateway* (p. 717)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	ec2:Region (p. 720)
EnableVolumeIO	Grants permission to enable I/O operations for a volume that had I/O operations disabled	Write	volume* (p. 717)	aws:ResourceTag/\${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:Encrypted (p. 718) ec2:ParentSnapshot (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:VolumeID (p. 722) ec2:VolumeIOPS (p. 722) ec2:VolumeSize (p. 722) ec2:VolumeThroughput (p. 722) ec2:VolumeType (p. 722)	ec2:Region (p. 720)
EnableVpcClassicLink	Grants permission to enable a VPC for ClassicLink	Write	vpc* (p. 714)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Tenancy (p. 722) ec2:VpcID (p. 722)	ec2:Region (p. 720)
EnableVpcClassicLinkToSupportDNSResolution	Grants permission to enable a VPC to support DNS hostname resolution for ClassicLink	Write	vpc (p. 714)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Tenancy (p. 722) ec2:VpcID (p. 722)	ec2:Region (p. 720)

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* (p. 692)	aws:ResourceTag/\${TagKey} (p. 717)	ec2:ClientRootCertificateChainArn (p. 718) ec2:CloudwatchLogGroupArn (p. 718) ec2:CloudwatchLogStreamArn (p. 718) ec2:DirectoryArn (p. 718) ec2:ResourceTag/\${TagKey} (p. 721) ec2:SamlProviderArn (p. 721) ec2:ServerCertificateArn (p. 721)
ExportClientVpnContent	Grants permission to download the contents of the Client VPN endpoint configuration file for a Client VPN endpoint	Read	client-vpn-endpoint* (p. 692)	aws:ResourceTag/\${TagKey} (p. 717)	ec2:ClientRootCertificateChainArn (p. 718) ec2:CloudwatchLogGroupArn (p. 718) ec2:CloudwatchLogStreamArn (p. 718) ec2:DirectoryArn (p. 718) ec2:ResourceTag/\${TagKey} (p. 721) ec2:SamlProviderArn (p. 721) ec2:ServerCertificateArn (p. 721)
ExportImage	Grants permission to export an Amazon Machine Image (AMI) to a VM file	Write	export-image-task* (p. 692)	aws:RequestTags/ \${TagKey} (p. 717) aws:TagKeys (p. 717)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			image* (p. 694) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ImageID (p. 718) ec2:ImageType (p. 718) ec2:Owner (p. 719) ec2:Public (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RootDeviceType (p. 721)		
			ec2:Region (p. 720)		
ExportTransitGatewayRoutesFromS3	Grants permission to export routes from a transit gateway route table to an Amazon S3 bucket	Write		ec2:Region (p. 720)	
GetAssociatedEncryptionCertificates	Grants permission to get the list of roles associated with an ACM certificate	Read	certificate* (p. 689)		
				ec2:Region (p. 720)	
GetAssociatedIpv6CidrInformation	Grants permission to get information about the IPv6 CIDR block associations for a specified IPv6 address pool	Read		ec2:Region (p. 720)	
GetCapacityReservationUsageInformation	Grants permission to get usage information about a Capacity Reservation	Read	capacity-reservation* (p. 789) aws:ResourceTag/ \${TagKey} (p. 717) ec2:CapacityReservationFleet (p. 718) ec2:ResourceTag/ \${TagKey} (p. 721)		
				ec2:Region (p. 720)	
GetCoipPoolUsage	Grants permission to describe the allocations from the specified customer-owned address pool	Read		ec2:Region (p. 720)	

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetConsoleOutput	Grants permission to get the console output for an instance	Read	instance* (p. 695) ResourceTag/\${TagKey} (p. 717)	ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceAutoRecovery (p. 719) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceMetadataTags (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:PlacementGroup (p. 720) ec2:ProductCode (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)	ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetConsoleScreenshot	Grants permission to retrieve a JPEG-format screenshot of a running instance	Read	instance (p. 696); ResourceTag/ \${TagKey} (p. 717)	ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceAutoRecovery (p. 719) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceMetadataTags (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:NewInstanceProfile (p. 719) ec2:PlacementGroup (p. 720) ec2:ProductCode (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)	ec2:Region (p. 720)
GetDefaultCredits	Grants permission to get the default credit option for CPU usage of a burstable performance instance family	Read		ec2:Region (p. 720)	
GetEbsDefaultKmId	Grants permission to get the ID of the default customer master key (CMK) for EBS encryption by default	Read		ec2:Region (p. 720)	
GetEbsEncryptionDefault	Grants permission to describe what EBS encryption by default is enabled for your account	Read		ec2:Region (p. 720)	

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetFlowLogsIntegrationCloudFormation	Grants permission to generate CloudFormation template to streamline the integration of VPC flow logs with Amazon Athena	Read	vpc-flow-log* (p. 713)	aws:ResourceTag/ {\$TagKey} (p. 717)	
				ec2:ResourceTag/ {\$TagKey} (p. 721)	
				ec2:Region (p. 720)	
GetGroupsForCapacityReservation	Grants permission to list the resource groups to which a Capacity Reservation has been added	List	capacity-reservation* (p. 718)	aws:ResourceTag/ {\$TagKey} (p. 717)	
				ec2:CapacityReservationFleet (p. 718)	
				ec2:ResourceTag/ {\$TagKey} (p. 721)	
GetHostReservationPurchasePreview	Grants permission to preview a host reservation purchase with configurations that match those of a Dedicated Host	Read		ec2:Region (p. 720)	
				ec2:Region (p. 720)	
GetInstanceTypesFilter	Grants permission to view a list of instance types with specified instance attributes	Read		ec2:Region (p. 720)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetInstanceUefiD	Grants permission to retrieve the binary representation of the UEFI variable store	Read	instance* (p. 695) ec2:ResourceTag/ \${TagKey} (p. 717)	ec2:AvailabilityZone (p. 718)	ec2:EbsOptimized (p. 718) ec2:InstanceAutoRecovery (p. 719) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceMetadataTags (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:NewInstanceProfile (p. 719) ec2:PlacementGroup (p. 720) ec2:ProductCode (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)
					ec2:Region (p. 720)
GetIpamAddressHistory	Grants permission to retrieve historical information about a CIDR within an Amazon VPC IP Address Manager (IPAM) scope	Read	ipam-scope* (p. 697) ec2:ResourceTag/ \${TagKey} (p. 721)	ec2:Region (p. 720)	
GetIpamPoolAllocation	Grants permission to get a list of all the CIDR allocations in an Amazon VPC IP Address Manager (IPAM) pool	Read	ipam-pool* (p. 697) ec2:ResourceTag/ \${TagKey} (p. 721)	ec2:Region (p. 720)	
GetIpamPoolCidrs	Grants permission to get the CIDRs provisioned to an Amazon VPC IP Address Manager (IPAM) pool	Read	ipam-pool* (p. 697) ec2:ResourceTag/ \${TagKey} (p. 721)	ec2:Region (p. 720)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetIpamResourceInformation	Grants permission to get information about the resources in an Amazon VPC IP Address Manager (IPAM) scope	Read	ipam-pool* (p. 697)	ec2:ResourceTag/\${TagKey} (p. 721)	
	ipam-scope* (p. 698)		ec2:ResourceTag/\${TagKey} (p. 721)		
				ec2:Region (p. 720)	
GetLaunchTemplateConfiguration	Grants permission to get the configuration data of the specified instance for use with a new launch template or launch template version	Read	instance* (p. 696)	ResourceTag/\${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceAutoRecovery (p. 719) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceMetadataTags (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:PlacementGroup (p. 720) ec2:ProductCode (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)	ec2:Region (p. 720)
GetManagedPrefixListInformation	Grants permission to get information about the resources that are associated with the specified managed prefix list	Read	prefix-list* (p. 704)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetManagedPrefixListInformation	Grants permission to get information about the entries for a specified managed prefix list	Read	prefix-list* (p. 704)	aws:ResourceTag/\${TagKey} (p. 717)	
	ec2:ResourceTag/\${TagKey} (p. 721)				
	ec2:Region (p. 720)				
GetNetworkInsightFindings	Grants permission to get the findings for Analysis Findings Network Access Scope analyses	Read			ec2:Region (p. 720)
GetNetworkInsightContent	Grants permission to get the contents for a specified Network Access Scope	Read			ec2:Region (p. 720)
GetPasswordData	Grants permission to retrieve the encrypted administrator password for a running Windows instance	Read	instance* (p. 696) aws:ResourceTag/\${TagKey} (p. 717)	ec2:AvailabilityZone (p. 718)	
ec2:EbsOptimized (p. 718)	ec2:InstanceAutoRecovery (p. 719)				
ec2:InstanceId (p. 719)	ec2:InstanceMarketType (p. 719)				
ec2:InstanceMetadataTags (p. 719)	ec2:InstanceProfile (p. 719)				
ec2:InstanceType (p. 719)	ec2:MetadataHttpEndpoint (p. 719)				
ec2:MetadataHttpPutResponseHopLimit (p. 719)	ec2:MetadataHttpTokens (p. 719)				
ec2:PlacementGroup (p. 720)	ec2:ProductCode (p. 720)				
ec2:ResourceTag/\${TagKey} (p. 721)	ec2:RootDeviceType (p. 721)				
ec2:Tenancy (p. 722)	ec2:Region (p. 720)				

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		ec2:Region (p. 720)	
GetResourcePolicy [permission only]	Grants permission to describe an IAM policy that enables cross-account sharing	Read	ipam-pool (p. 697) \${TagKey} (p. 721)	ec2:ResourceTag/	
			ec2:Region (p. 720)		
GetSerialConsoleStatus	Grants permission to retrieve the access status of your account to the EC2 serial console of all instances	Read		ec2:Region (p. 720)	
GetSpotPlacementScore	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 (p. 720)	
GetSubnetCidrReservationInformation	Grants permission to retrieve information about the subnet CIDR reservations	Read		ec2:Region (p. 720)	
GetTransitGatewayRouteTables	Grants permission to list the route tables to which a resource attachment propagates routes	List		ec2:Region (p. 720)	
GetTransitGatewayMulticastDomainAssociations	Grants permission to get information about the associations for a transit gateway multicast domain	List		ec2:Region (p. 720)	
GetTransitGatewayPrefixListReferences	Grants permission to get information about prefix list references for a transit gateway route table	List		ec2:Region (p. 720)	
GetTransitGatewayRouteTableAssociations	Grants permission to get information about associations for a transit gateway route table	List		ec2:Region (p. 720)	
GetTransitGatewayRouteTablePropagations	Grants permission to get information about the route table propagations for a transit gateway route table	List		ec2:Region (p. 720)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetVpnConnection <small>Grants permission to download an AWS provided sample configuration file to be used with the customer gateway device</small>		List	vpn-connection*	aws:ResourceTag/ {\$TagKey} (p. 717)	
			vpn-connection-device-type (p. 715)	ec2:ResourceTag/ {\$TagKey} (p. 721)	
					ec2:Region (p. 720)
GetVpnConnection <small>Grants permission to obtain a list of customer gateway devices for which sample configuration files can be provided</small>		List			ec2:Region (p. 720)
ImportClientVpnClientCertificateRevocationList <small>Grants permission to upload a Client Certificate Revocation List to a Client VPN endpoint</small>		Write	client-vpn-endpoint*	aws:ResourceTag/ {\$TagKey} (p. 717)	
		ec2:ClientRootCertificateChainArn (p. 718)			
		ec2:CloudwatchLogGroupArn (p. 718)			
		ec2:CloudwatchLogStreamArn (p. 718)			
		ec2:DirectoryArn (p. 718)			
		ec2:ResourceTag/ {\$TagKey} (p. 721)			
		ec2:SamlProviderArn (p. 721)			
		ec2:ServerCertificateArn (p. 721)			
		ec2:Region (p. 720)			
ImportImage <small>Grants permission to import single or multi-volume disk images or EBS snapshots into an Amazon Machine Image (AMI)</small>		Write	image* (p. 694)	aws:RequesterCreateTags/ {\$TagKey} (p. 717)	
		aws:TagKeys (p. 717)			
		ec2:ImageID (p. 718)			
		ec2:ImageType (p. 718)			
		ec2:Owner (p. 719)			
		ec2:Public (p. 720)			
		ec2:RootDeviceType (p. 721)			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			import-image-task* (p. 694) snapshot (p. 707)	aws:RequestTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) aws:ResourceTag/\${TagKey} (p. 717) ec2:Owner (p. 719) ec2:ParentVolume (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:SnapshotID (p. 721) ec2:SnapshotTime (p. 721) ec2:VolumeSize (p. 722)	
ImportInstance	Grants permission to create an import instance task using metadata from a disk image	Write	instance* (p. 696) volume* (p. 710)	aws:ResourceTag/\${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:InstanceId (p. 719) ec2:ResourceTag/\${TagKey} (p. 721)	aws:ResourceTag/\${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:Encrypted (p. 718) ec2:ParentSnapshot (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:VolumeID (p. 722) ec2:VolumeIops (p. 722) ec2:VolumeSize (p. 722) ec2:VolumeThroughput (p. 722) ec2:VolumeType (p. 722)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			security-group (p. 705) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SecurityGroupID (p. 721) ec2:Vpc (p. 722)		aws:ResourceTag/ \${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SubnetID (p. 722) ec2:Vpc (p. 722)
			subnet (p. 709) aws:ResourceTag/ \${TagKey} (p. 717) ec2:Region (p. 720)		aws:ResourceTag/ \${TagKey} (p. 717) ec2:Region (p. 720)
ImportKeyPair	Grants permission to import a public key from an RSA key pair that was created with a third-party tool	Write	key-pair* (p. 699) aws:RequestTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717)		aws:RequestTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720)
ImportSnapshot	Grants permission to import a disk into an EBS snapshot	Write	import-snapshot-task* (p. 694) snapshot* (p. 707) aws:RequestTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Owner (p. 719) ec2:ParentVolume (p. 720) ec2:SnapshotID (p. 721) ec2:SnapshotTime (p. 721) ec2:VolumeSize (p. 722)		aws:RequestTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720)

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* (p. 720) aws:ResourceTag/ \${TagKey} (p. 717)	ec2:AvailabilityZone (p. 718) ec2:Encrypted (p. 718) ec2:ParentSnapshot (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:VolumeID (p. 722) ec2:VolumeIops (p. 722) ec2:VolumeSize (p. 722) ec2:VolumeThroughput (p. 722) ec2:VolumeType (p. 722)	ec2:Region (p. 720)
	ec2:Region (p. 720)				
ListImagesInRecycleBin	Grants permission to list Amazon Machine Images (AMIs) that are currently in the Recycle Bin	List	image (p. 694) aws:ResourceTag/ \${TagKey} (p. 717)	ec2:ImageID (p. 718) ec2:ImageType (p. 718) ec2:Owner (p. 719) ec2:Public (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RootDeviceType (p. 721)	ec2:Region (p. 720)
	ec2:Region (p. 720)				

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListSnapshotsInRecycleBin	Grants permission to list the Amazon EBS snapshots that are currently in the Recycle Bin	List	snapshot (p. 207) aws:ResourceTag/ \${TagKey} (p. 717)	ec2:AvailabilityZone (p. 718) ec2:Encrypted (p. 718) ec2:Owner (p. 719) ec2:ParentVolume (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SnapshotID (p. 721) ec2:SnapshotTime (p. 721) ec2:VolumeSize (p. 722)	ec2:Region (p. 720)
ModifyAddressAttribute	Grants permission to modify an attribute of the specified Elastic IP address	Write	elastic-ip* (p. 687)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:AllocationId (p. 717) ec2:Attribute (p. 717) ec2:Attribute/ \${AttributeName} (p. 717) ec2:Domain (p. 718) ec2:PublicIpAddress (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721)	ec2:Region (p. 720)
ModifyAvailabilityOptions	Grants permission to modify the option status s of the Local Zone and Wavelength Zone group for your account	Write			ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:CapacityReservationFleet (p. 718) ec2:ResourceTag/\${TagKey} (p. 721)	
				ec2:Region (p. 720)	
ModifyCapacityReservationFleet	Grants permission to modify a Capacity Reservation Fleet	Write	capacity-reservation-fleet* (p. 688)	aws:ResourceTag/\${TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
				ec2:Region (p. 720)	
ModifyClientVpnEndpoint	Grants permission to modify a Client VPN endpoint	Write	client-vpn-endpoint* (p. 689)	aws:ResourceTag/\${TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:ClientRootCertificateChainArn (p. 718) ec2:CloudwatchLogGroupArn (p. 718) ec2:CloudwatchLogStreamArn (p. 718) ec2:DirectoryArn (p. 718) ec2:ResourceTag/\${TagKey} (p. 721) ec2:SamlProviderArn (p. 721) ec2:ServerCertificateArn (p. 721)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			security-group (p. 705) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SecurityGroupID (p. 721)		
	vpc (p. 714) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:VpcID (p. 722)				
				ec2:Region (p. 720)	
ModifyDefaultCreditType	Grants permission to change the Specified level default credit option for CPU usage of burstable performance instances	Write			ec2:Region (p. 720)
ModifyEbsDefaultCustomerMasterKey	Grants permission to change the default customer master key (CMK) for EBS encryption by default for your account	Write			ec2:Region (p. 720)
ModifyFleet	Grants permission to modify an EC2 Fleet	Write	fleet* (p. 692) aws:ResourceTag/ \${TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/ \${AttributeName} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		
image (p. 694) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ImageID (p. 718) ec2:ImageType (p. 718) ec2:Owner (p. 719) ec2:Public (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RootDeviceType (p. 721)					

Service Authorization Reference
 Service Authorization Reference
 Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			key-pair (p. 699)	aws:ResourceTag/\${TagKey} (p. 717) ec2:KeyPairName (p. 719) ec2:ResourceTag/\${TagKey} (p. 721)	
			launch-template (p. 699)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			network-interface (p. 703)	aws:ResourceTag/\${TagKey} (p. 717) ec2:AssociatePublicIpAddress (p. 717) ec2:AuthorizedService (p. 717) ec2:AvailabilityZone (p. 718) ec2:NetworkInterfaceID (p. 719) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Subnet (p. 721) ec2:Vpc (p. 722)	
			security-group (p. 705)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	ec2:SecurityGroupID (p. 721) ec2:Vpc (p. 722)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot (p. 207) aws:ResourceTag/ \${TagKey} (p. 717) ec2:Owner (p. 719) ec2:ParentVolume (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SnapshotID (p. 721) ec2:SnapshotTime (p. 721) ec2:VolumeSize (p. 722)		
	subnet (p. 709) aws:ResourceTag/ \${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SubnetID (p. 722) ec2:Vpc (p. 722)				
				ec2:Region (p. 720)	
ModifyFpgaImageAttribute	Grants permission to modify an attribute of an Amazon FPGA Image (AFI)	Write	fpga-image* (p. 69) aws:ResourceTag/ \${TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/ \${AttributeName} (p. 717) ec2:Owner (p. 719) ec2:Public (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721)		aws:ResourceTag/ \${TagKey} (p. 717) ec2:Region (p. 720)
ModifyHosts	Grants permission to modify a Dedicated Host	Write	dedicated-host* (p. 69) aws:ResourceTag/ \${TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/ \${AttributeName} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:Region (p. 720)
ModifyIdFormat	Grants permission to modify the ID format for a resource	Write			ec2:Region (p. 720)
ModifyIdentityIdFormat	Grants permission to modify the ID format of a resource for a specific principal in your account	Write			ec2:Region (p. 720)
ModifyImageAttribute	Grants permission to modify an attribute of an Amazon Machine Image (AMI)	Write	image* (p. 694) aws:ResourceTag/\${TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:ImageID (p. 718) ec2:ImageType (p. 718) ec2:Owner (p. 719) ec2:Public (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RootDeviceType (p. 721)	ec2:Region (p. 720)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstanceAttribute	Grants permission to modify an attribute of an instance	Write	instance* (p. 695) aws:ResourceTag/ \${TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/ \${AttributeName} (p. 717) ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceAutoRecovery (p. 719) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceMetadataTags (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLim ec2:MetadataHttpTokens (p. 719) ec2:PlacementGroup (p. 720) ec2:ProductCode (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)		
			security-group (p. 705) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SecurityGroupID (p. 721) ec2:Vpc (p. 722)		

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume (p. 717) aws:ResourceTag/\${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:Encrypted (p. 718) ec2:ParentSnapshot (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:VolumeID (p. 722) ec2:VolumeIops (p. 722) ec2:VolumeSize (p. 722) ec2:VolumeThroughput (p. 722) ec2:VolumeType (p. 722)		ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstanceCapacityReservationSettings	<p>Grants permission to modify the Capacity Reservation settings for a stopped instance</p>	Write	<p>instance* (p. 695)</p> <p>ResourceTag/ \${TagKey} (p. 717)</p> <p>ec2:Attribute (p. 717)</p> <p>ec2:Attribute/ \${AttributeName} (p. 717)</p> <p>ec2:AvailabilityZone (p. 718)</p> <p>ec2:EbsOptimized (p. 718)</p> <p>ec2:InstanceAutoRecovery (p. 719)</p> <p>ec2:InstanceId (p. 719)</p> <p>ec2:InstanceMarketType (p. 719)</p> <p>ec2:InstanceMetadataTags (p. 719)</p> <p>ec2:InstanceProfile (p. 719)</p> <p>ec2:InstanceType (p. 719)</p> <p>ec2:MetadataHttpEndpoint (p. 719)</p> <p>ec2:MetadataHttpPutResponseHopLimit (p. 719)</p> <p>ec2:MetadataHttpTokens (p. 719)</p> <p>ec2:PlacementGroup (p. 720)</p> <p>ec2:ProductCode (p. 720)</p> <p>ec2:ResourceTag/ \${TagKey} (p. 721)</p> <p>ec2:RootDeviceType (p. 721)</p> <p>ec2:Tenancy (p. 722)</p>	<p>aws:ResourceTag/ \${TagKey} (p. 717)</p> <p>ec2:ResourceTag/ \${TagKey} (p. 721)</p>	<p>ec2:Region (p. 720)</p>

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstanceCreditSpecification	Grants permission to modify the CPU usage on an instance	Write	instance* (p. 696) ResourceTag/ {\$TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/ {\$AttributeName} (p. 717) ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceAutoRecovery (p. 719) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceMetadataTags (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:PlacementGroup (p. 720) ec2:ProductCode (p. 720) ec2:ResourceTag/ {\$TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)		ec2:Region (p. 720)
ModifyInstanceEventStartTime	Grants permission to modify the start time for a scheduled EC2 instance event	Write	instance* (p. 696) ResourceTag/ {\$TagKey} (p. 717) ec2:Attribute/ {\$AttributeName} (p. 717) ec2:InstanceId (p. 719) ec2:ResourceTag/ {\$TagKey} (p. 721)		ec2:Region (p. 720)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions	
ModifyInstanceEventWindow	Grants permission to modify the specified event window	Write	instance-event-window* (p. 695)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)		
				ec2:Region (p. 720)		
ModifyInstanceMetadataRecoveryBehavior	Grants permission to modify the recovery behaviour for an instance	Write	instance* (p. 696)	aws:ResourceTag/\${TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceAutoRecovery (p. 719) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceMetadataTags (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:PlacementGroup (p. 720) ec2:ProductCode (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)		
	ec2:Region (p. 720)					

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstanceMetadata	<p>Grants permission to modify the instance metadata options for an instance</p>	Write	instance* (p. 695) ResourceTag/\${TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceAutoRecovery (p. 719) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceMetadataTags (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:PlacementGroup (p. 720) ec2:ProductCode (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)	695 ResourceTag/\${TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceAutoRecovery (p. 719) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceMetadataTags (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:PlacementGroup (p. 720) ec2:ProductCode (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)	ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstancePlacement	Grants permission to modify the placement attributes for an instance	Write	instance* (p. 695) aws:ResourceTag/ \${TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/ \${AttributeName} (p. 717) ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceAutoRecovery (p. 719) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceMetadataTags (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLim ec2:MetadataHttpTokens (p. 719) ec2:PlacementGroup (p. 720) ec2:ProductCode (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)		
		dedicated-host (p. 690)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		
		placement-group (p. 703)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:PlacementGroupName (p. 720) ec2:PlacementGroupStrategy (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721)		

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:Region (p. 720)
ModifyIpam	Grants permission to modify the configurations of an Amazon VPC IP Address Manager (IPAM)	Write	ipam* (p. 697) ec2:Attribute (p. 717) ec2:Attribute/ {\$AttributeName} (p. 717) ec2:ResourceTag/ {\$TagKey} (p. 721)		ec2:Region (p. 720)
					ec2:Region (p. 720)
ModifyIpamPool	Grants permission to modify the configurations of an Amazon VPC IP Address Manager (IPAM) pool	Write	ipam- pool* (p. 697) ec2:Attribute (p. 717) ec2:Attribute/ {\$AttributeName} (p. 717) ec2:ResourceTag/ {\$TagKey} (p. 721)		ec2:Region (p. 720)
					ec2:Region (p. 720)
ModifyIpamResource	Grants permission to modify the configurations of an Amazon VPC IP Address Manager (IPAM) resource CIDR	Write	ipam- scope* (p. 698) ec2:Attribute (p. 717) ec2:Attribute/ {\$AttributeName} (p. 717) ec2:ResourceTag/ {\$TagKey} (p. 721)		ec2:Region (p. 720)
					ec2:Region (p. 720)
ModifyIpamScope	Grants permission to modify the configurations of an Amazon VPC IP Address Manager (IPAM) scope	Write	ipam- scope* (p. 698) ec2:Attribute (p. 717) ec2:Attribute/ {\$AttributeName} (p. 717) ec2:ResourceTag/ {\$TagKey} (p. 721)		ec2:Region (p. 720)
					ec2:Region (p. 720)
ModifyLaunchTemplate	Grants permission to modify a launch template	Write	launch- template* (p. 699) aws:ResourceTag/ {\$TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/ {\$AttributeName} (p. 717) ec2:ResourceTag/ {\$TagKey} (p. 721)		aws:ResourceTag/ {\$TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/ {\$AttributeName} (p. 717) ec2:ResourceTag/ {\$TagKey} (p. 721)
					ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyManagedPrefixList*	Grants permission to modify a managed prefix list	Write	prefix-list* (p. 704)	aws:ResourceTag/\${TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
			ec2:Region (p. 720)		
ModifyNetworkInterfaceAttribute*	Grants permission to modify an attribute of a network interface	Write	network-interface* (p. 704)	aws:ResourceTag/\${TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:AvailabilityZone (p. 718) ec2:NetworkInterfaceID (p. 719) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Subnet (p. 721) ec2:Vpc (p. 722)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance (p. 636) aws:ResourceTag/ \${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceAutoRecovery (p. 719) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceMetadataTags (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:PlacementGroup (p. 720) ec2:ProductCode (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)		
			security-group (p. 705) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SecurityGroupID (p. 721) ec2:Vpc (p. 722)		
					ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyPrivateDnsOptionsForInstances	Grants permission to modify the option\$for\$instances for the specified instance	Write	instance* (p. 695) ResourceTag/ {\$TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/ {\$AttributeName} (p. 717) ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceAutoRecovery (p. 719) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceMetadataTags (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLim ec2:MetadataHttpTokens (p. 719) ec2:NewInstanceProfile (p. 719) ec2:PlacementGroup (p. 720) ec2:ProductCode (p. 720) ec2:ResourceTag/ {\$TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)		ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyReservedInstancesAttribute	Grants permission to modify attributes of one or more Reserved Instances	Write	reserved-instances* (p. 704)	aws:ResourceTag/\${TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:AvailabilityZone (p. 718) ec2:InstanceType (p. 719) ec2:ReservedInstancesOfferingType (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Tenancy (p. 722)	aws:ResourceTag/\${TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:AvailabilityZone (p. 718) ec2:InstanceType (p. 719) ec2:ReservedInstancesOfferingType (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Tenancy (p. 722)
	ec2:Region (p. 720)				
ModifySecurityGroupRule	Grants permission to modify the ruleRole security group	Write	security-group* (p. 704)	aws:ResourceTag/\${TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721) ec2:SecurityGroupID (p. 721) ec2:Vpc (p. 722)	aws:ResourceTag/\${TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721) ec2:SecurityGroupID (p. 721) ec2:Vpc (p. 722)
	prefix-list (p. 704)		aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)		
	security-group-rule (p. 706)		aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)		
	ec2:Region (p. 720)				

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* (p. 705) ResourceTag/ \${TagKey} (p. 717)		ec2:Add/group (p. 717) ec2:Add/userId (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:Owner (p. 719) ec2:ParentVolume (p. 720) ec2:Remove/group (p. 721) ec2:Remove/userId (p. 721) ec2:ResourceTag/\${TagKey} (p. 721) ec2:SnapshotID (p. 721) ec2:SnapshotTime (p. 721) ec2:VolumeSize (p. 722)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifySnapshotTags	Grants permission to archive Amazon EBS snapshots	Write	snapshot* (p. 705) aws:ResourceTag/ \${TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/ \${AttributeName} (p. 717) ec2:AvailabilityZone (p. 718) ec2:Encrypted (p. 718) ec2:Owner (p. 719) ec2:ParentVolume (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SnapshotID (p. 721) ec2:SnapshotTime (p. 721) ec2:VolumeSize (p. 722)		ec2:Region (p. 720)
ModifySpotFleetRequests	Grants permission to modify a SpotFleet request	Write	spot-fleet-request* (p. 708) aws:ResourceTag/ \${TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/ \${AttributeName} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifySubnetAttribute	Grants permission to modify an attribute of a subnet	Write	subnet* (p. 709) aws:ResourceTag/ \${TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/ \${AttributeName} (p. 717) ec2:AvailabilityZone (p. 718) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SubnetID (p. 722) ec2:Vpc (p. 722)		ec2:Region (p. 720)
ModifyTrafficMirrorFilterRule	Grants permission to allow or restrict traffic mirroring in network services	Write	traffic-mirror-filter* (p. 709) aws:ResourceTag/ \${TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/ \${AttributeName} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		ec2:Region (p. 720)
ModifyTrafficMirrorRule	Grants permission to modify a traffic mirror rule	Write	traffic-mirror-filter* (p. 709) aws:ResourceTag/ \${TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/ \${AttributeName} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)	ec2:Attribute (p. 717) ec2:Attribute/ \${AttributeName} (p. 717)	ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyTrafficMirrorSession	Grants permission to modify a traffic mirror session	Write	traffic-mirror-session* (p. 710)	aws:ResourceTag/\${TagKey} (p. 717) ec2:Attribute (p. 717)	ec2:Attribute/\${AttributeName} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)
	traffic-mirror-filter (p. 709)		aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)		
	traffic-mirror-target (p. 710)		aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)		
				ec2:Region (p. 720)	
ModifyTransitGateway	Grants permission to modify a transit gateway	Write	transit-gateway* (p. 711)	aws:ResourceTag/\${TagKey} (p. 717) ec2:Attribute (p. 717)	ec2:Attribute/\${AttributeName} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)
	transit-gateway-route-table (p. 712)		aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)		
				ec2:Region (p. 720)	
ModifyTransitGatewayPrefixListReference	Grants permission to modify a transit gateway prefixlist reference	Write	prefix-list* (p. 704)	aws:ResourceTag/\${TagKey} (p. 717) ec2:Attribute (p. 717)	ec2:Attribute/\${AttributeName} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-route-table* (p. 710)	aws:ResourceTag/\${TagKey} (p. 717) ec2:Attribute (p. 717)	ec2:Attribute/\${AttributeName} (p. 717)
	transit-gateway-attachment		aws:ResourceTag/\${TagKey} (p. 717)	ec2:ResourceTag/\${TagKey} (p. 721)	
			ec2:Region (p. 720)		
ModifyTransitGatewayVpcAttachment	Grants permission to modify AVC attachment on a transit gateway	Write	transit-gateway-attachment*	aws:ResourceTag/\${TagKey} (p. 717) (p. 710) ec2:Attribute (p. 717)	ec2:Attribute/\${AttributeName} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)
			subnet (p. 709)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	ec2:SubnetID (p. 722)
					ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVolume	Grants permission to modify the parameters of an EBS volume	Write	volume* (p. 710); \${ResourceTag}/ \${TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/ \${AttributeName} (p. 717) ec2:AvailabilityZone (p. 718) ec2:Encrypted (p. 718) ec2:ParentSnapshot (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:VolumeID (p. 722) ec2:VolumeIops (p. 722) ec2:VolumeSize (p. 722) ec2:VolumeThroughput (p. 722) ec2:VolumeType (p. 722)		ec2:Region (p. 720)
ModifyVolumeAttribute	Grants permission to modify an attribute of a volume	Write	volume* (p. 710); \${ResourceTag}/ \${TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/ \${AttributeName} (p. 717) ec2:AvailabilityZone (p. 718) ec2:Encrypted (p. 718) ec2:ParentSnapshot (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:VolumeID (p. 722) ec2:VolumeIops (p. 722) ec2:VolumeSize (p. 722) ec2:VolumeThroughput (p. 722) ec2:VolumeType (p. 722)		ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions	
ModifyVpcAttribute	Grants permission to modify an attribute of a VPC	Write	vpc* (p. 714)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/ \${AttributeName} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:Tenancy (p. 722) ec2:VpcID (p. 722)		
					ec2:Region (p. 720)	
ModifyVpcEndpointAttribute	Grants permission to modify an attribute of a VPC endpoint	Write	vpc- endpoint* (p. 705)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/ \${AttributeName} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		
				route- table (p. 705)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RouteTableID (p. 721)	
				security- group (p. 705)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SecurityGroupID (p. 721)	
				subnet (p. 705)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SubnetID (p. 722)	
						ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVpcEndpointConnectionNotification	Grants permission to modify connection notification for a VPC endpoint or VPC endpoint service	Write	vpc-endpoint* (p. 713) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	aws:ResourceTag/\${TagKey} (p. 717)	
	vpc-endpoint-service* (p. 713) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)		aws:ResourceTag/\${TagKey} (p. 717)	ec2:Attribute (p. 717)	
				ec2:Region (p. 720)	
ModifyVpcEndpointConfiguration	Grants permission to modify the configuration of a VPC endpoint service configuration	Write	vpc-endpoint-service* (p. 713) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	aws:ResourceTag/\${TagKey} (p. 717)	ec2:VpceServicePrivateDnsName (p. 720)
				ec2:Region (p. 720)	
ModifyVpcEndpointPayPerRequest	Grants permission to modify the pay per request responsibility for a VPC endpoint service	Write	vpc-endpoint-service* (p. 713) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	aws:ResourceTag/\${TagKey} (p. 717)	ec2:VpceServicePrivateDnsName (p. 720)
				ec2:Region (p. 720)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVpcEndpointPermissionsForAVPC	Grants permission to modify the permissions for a VPC endpoint service	Permissions management	vpc-endpoint-service* (p. 713)	aws:ResourceTag/ {\$TagKey} (p. 717)	ec2:Attribute (p. 717) ec2:Attribute/ {\$AttributeName} (p. 717) ec2:ResourceTag/ {\$TagKey} (p. 721)
				ec2:Region (p. 720)	
ModifyVpcPeeringOptions	Grants permission to modify the VPC peering options on one side of a VPC peering connection	Write	vpc-peering-connection* (p. 714)	aws:ResourceTag/ {\$TagKey} (p. 717)	ec2:AccepterVpc (p. 717) ec2:Attribute (p. 717) ec2:Attribute/ {\$AttributeName} (p. 717) ec2:RequesterVpc (p. 721) ec2:ResourceTag/ {\$TagKey} (p. 721)
				ec2:VpcPeeringConnectionID (p. 722)	
ModifyVpcTenancy	Grants permission to modify the instance tenancy attribute of a VPC	Write	vpc* (p. 714)	aws:ResourceTag/ {\$TagKey} (p. 717)	ec2:Attribute (p. 717) ec2:Attribute/ {\$AttributeName} (p. 717) ec2:ResourceTag/ {\$TagKey} (p. 721)
				ec2:Tenancy (p. 722) ec2:VpcID (p. 722)	
					ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVpnConnectionTarget	Grants permission to modify the target gateway of a Site-to-Site VPN connection	Write	vpn-connection*	aws:ResourceTag/\${TagKey} (p. 718) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:AuthenticationType (p. 717) ec2:DPDTimeoutSeconds (p. 718) ec2:GatewayType (p. 718) ec2:IKEVersions (p. 718) ec2:InsideTunnelCidr (p. 718) ec2:InsideTunnelIpv6Cidr (p. 718) ec2:Phase1DHGroup (p. 720) ec2:Phase1EncryptionAlgorithms (p. 720) ec2:Phase1IntegrityAlgorithms (p. 720) ec2:Phase1LifetimeSeconds (p. 720) ec2:Phase2DHGroup (p. 720) ec2:Phase2EncryptionAlgorithms (p. 720) ec2:Phase2IntegrityAlgorithms (p. 720) ec2:Phase2LifetimeSeconds (p. 720) ec2:PreSharedKeys (p. 720) ec2:RekeyFuzzPercentage (p. 721) ec2:RekeyMarginTimeSeconds (p. 721) ec2:ReplayWindowSizePackets (p. 721) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RoutingType (p. 721)	ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVpnConnection	Grants permission to modify the connection options for your Site-to-Site VPN connection	Write	vpn-connection*	aws:ResourceTag/\${TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
	ec2:Region (p. 720)				
ModifyVpnTunnelCertificate	Grants permission to modify the certificate for a Site-to-Site VPN connection	Write	vpn-connection*	aws:ResourceTag/\${TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
	ec2:Region (p. 720)				

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} (p. 718) ec2:Attribute (p. 717) ec2:Attribute/ \${AttributeName} (p. 717) ec2:AuthenticationType (p. 717) ec2:DPDTTimeoutSeconds (p. 718) ec2:GatewayType (p. 718) ec2:IKEVersions (p. 718) ec2:InsideTunnelCidr (p. 718) ec2:InsideTunnelIpv6Cidr (p. 718) ec2:Phase1DHGroup (p. 720) ec2:Phase1EncryptionAlgorithms (p. 720) ec2:Phase1IntegrityAlgorithms (p. 720) ec2:Phase1LifetimeSeconds (p. 720) ec2:Phase2DHGroup (p. 720) ec2:Phase2EncryptionAlgorithms (p. 720) ec2:Phase2IntegrityAlgorithms (p. 720) ec2:Phase2LifetimeSeconds (p. 720) ec2:PreSharedKeys (p. 720) ec2:RekeyFuzzPercentage (p. 721) ec2:RekeyMarginTimeSeconds (p. 721) ec2:ReplayWindowSizePackets (p. 721) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RoutingType (p. 721)	ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
MonitorInstances	Grants permission to enable detailed monitoring for a running instance	Write	instance* (p. 695)	ResourceTag/ \${TagKey} (p. 717)	ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceAutoRecovery (p. 719) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceMetadataTags (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:PlacementGroup (p. 720) ec2:ProductCode (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)
					ec2:Region (p. 720)
MoveAddressToVpc	Grants permission to move an Elastic IP address from the EC2-Classic platform to the EC2-VPC platform	Write			ec2:Region (p. 720)
MoveByoipCidrToIpam	Grants permission to move a BYOIP IPv4 CIDR to Amazon VPC IP Address Manager (IPAM) from a public IPv4 pool	Write	ipam-pool (p. 697)	ec2:ResourceTag/ \${TagKey} (p. 721)	
					ec2:Region (p. 720)
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 (p. 720)
ProvisionIpamPoolCidr	Grants permission to provision a CIDR to an Amazon VPC IP Address Manager (IPAM) pool	Write	ipam-pool* (p. 697)	ec2:ResourceTag/ \${TagKey} (p. 721)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:Region (p. 720)
ProvisionPublicIPv4CidrBlock	Grants permission to provision a public IPv4 pool	Write	ipam-pool* (p. 697)	ec2:ResourceTag/\${TagKey} (p. 721)	
			ipv4pool-ec2 (p. 698)	aws:ResourceTag/\${TagKey} (p. 717)	
				ec2:ResourceTag/\${TagKey} (p. 721)	
					ec2:Region (p. 720)
PurchaseHostReservation	Grants permission to purchase a reservation with configurations that match those of a Dedicated Host	Write	dedicated-host* (p. 690)	aws:ResourceTag/\${TagKey} (p. 717)	
				ec2:ResourceTag/\${TagKey} (p. 721)	
					ec2:Region (p. 720)
PurchaseReservedInstancesOffering	Grants permission to purchase a Reserved Instance offering	Write			ec2:Region (p. 720)
PurchaseScheduledInstances	Grants permission to purchase one or more Scheduled Instances with a specified schedule	Write			ec2:Region (p. 720)
PutResourcePolicy [permission only]	Grants permission to attach an IAM policy that enables cross-account sharing to a resource	Write	ipam-pool (p. 697)	ec2:ResourceTag/\${TagKey} (p. 721)	
					ec2:Region (p. 720)

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* (p. 695) aws:ResourceTag/\${TagKey} (p. 717)	ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceAutoRecovery (p. 719) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceMetadataTags (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:PlacementGroup (p. 720) ec2:ProductCode (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)	ec2:Region (p. 720)
RegisterImage	Grants permission to register an Amazon Machine Image (AMI)	Write	image* (p. 694) aws:ResourceTag/\${TagKey} (p. 717)	ec2:ImageID (p. 718) ec2:Owner (p. 719) ec2:ResourceTag/\${TagKey} (p. 721)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot (p. 207) aws:ResourceTag/ \${TagKey} (p. 717) ec2:OutpostArn (p. 719) ec2:Owner (p. 719) ec2:ParentVolume (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SnapshotID (p. 721) ec2:SnapshotTime (p. 721) ec2:SourceOutpostArn (p. 721) ec2:VolumeSize (p. 722)		ec2:Region (p. 720)
RegisterInstanceEventNotification	Grants permission to add tags to the set of tags to include in notifications about scheduled events for your instances	Write			ec2:Region (p. 720)
RegisterTransitGatewayMulticastDomainMember	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* (p. 705) aws:ResourceTag/ \${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:NetworkInterfaceID (p. 719) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:Subnet (p. 721) ec2:Vpc (p. 722)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:NetworkInterfaceID (p. 719) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:Subnet (p. 721) ec2:Vpc (p. 722)	ec2:Region (p. 720)
transit-gateway-multicast-domain* (p. 702) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)	ec2:Region (p. 720)				
	ec2:Region (p. 720)				

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterTransitGatewayNetworkInterface	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* (p. 710)	aws:ResourceTag/\${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:NetworkInterfaceID (p. 719) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Subnet (p. 721) ec2:Vpc (p. 722)	
	transit-gateway-multicast-domain* (p. 710)		aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)		
				ec2:Region (p. 720)	
RejectTransitGatewayMulticastDomainAttachmentRequest	Grants permission to reject requests to associate cross-account subnets with a transit gateway multicast domain	Write	transit-gateway-attachment (p. 710)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
	transit-gateway-multicast-domain (p. 710)		aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)		
				ec2:Region (p. 720)	
RejectTransitGatewayPeeringAttachmentRequest	Grants permission to reject a transit gateway peering attachment request	Write	transit-gateway-attachment* (p. 710)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
				ec2:Region (p. 720)	
RejectTransitGatewayVpcAttachmentRequest	Grants permission to reject a request to attach a VPC to a transit gateway	Write	transit-gateway-attachment* (p. 710)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	
				ec2:Region (p. 720)	

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RejectVpcEndpointConnection	Grants permission to reject one or more VPC endpoint connection requests to a VPC endpoint service	Write	vpc-endpoint-service* (p. 713)	aws:ResourceTag/\${TagKey} (p. 717)	ec2:ResourceTag/\${TagKey} (p. 721)
				ec2:Region (p. 720)	
RejectVpcPeeringConnection	Grants permission to reject a VPC peering connection request	Write	vpc-peering-connection*	aws:ResourceTag/\${TagKey} (p. 717)	ec2:AcceptorVpc (p. 717)
				ec2:RequesterVpc (p. 721)	
				ec2:ResourceTag/\${TagKey} (p. 721)	
ReleaseAddress	Grants permission to release an Elastic IP address	Write	elastic-ip (p. 687)	aws:ResourceTag/\${TagKey} (p. 717)	ec2:AllocationId (p. 717)
				ec2:Domain (p. 718)	
ReleaseHosts	Grants permission to release one or more On-Demand Dedicated Hosts	Write	dedicated-host* (p. 690)	aws:ResourceTag/\${TagKey} (p. 717)	ec2:ResourceTag/\${TagKey} (p. 721)
				ec2:Region (p. 720)	
				ec2:Region (p. 720)	
ReleaseIpamPoolAllocation	Grants permission to release an allocation within an Amazon VPC IP Address Manager (IPAM) pool	Write	ipam-pool* (p. 697)	ec2:ResourceTag/\${TagKey} (p. 721)	ec2:Region (p. 720)
				ec2:Region (p. 720)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ReplaceIamInstanceProfile	Grants permission to replace the IAM instance profile for an instance	Write	instance* (p. 695) aws:ResourceTag/\${TagKey} (p. 717)	iam:PassRole	ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceAutoRecovery (p. 719) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceMetadataTags (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:NewInstanceProfile (p. 719) ec2:PlacementGroup (p. 720) ec2:ProductCode (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)
ReplaceNetworkAcl	Grants permission to change which network ACL a subnet is associated with	Write	network-acl* (p. 701)	aws:ResourceTag/\${TagKey} (p. 717)	ec2:NetworkAclID (p. 719) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Vpc (p. 722)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet* (p. 709) aws:ResourceTag/ \${TagKey} (p. 717)	ec2:AvailabilityZone (p. 718)	ec2:ResourceTag/ \${TagKey} (p. 721)
	ec2:SubnetID (p. 722)		ec2:Vpc (p. 722)	ec2:Region (p. 720)	
ReplaceNetworkAclEntry	Grants permission to replace an entry (rule) in a network ACL	Write	network-acl* (p. 701) aws:ResourceTag/ \${TagKey} (p. 717)	ec2:NetworkAclID (p. 719)	ec2:ResourceTag/ \${TagKey} (p. 721)
	ec2:Vpc (p. 722)		ec2:Region (p. 720)		
ReplaceRoute	Grants permission to replace a route within a route table in a VPC	Write	route-table* (p. 705) aws:ResourceTag/ \${TagKey} (p. 717)	ec2:ResourceTag/ \${TagKey} (p. 721)	ec2:RouteTableID (p. 721)
	carrier-gateway (p. 689) aws:ResourceTag/ \${TagKey} (p. 717)		ec2:ResourceTag/ \${TagKey} (p. 721)	ec2:Tenancy (p. 722)	
	egress-only-internet-gateway (p. 692) aws:ResourceTag/ \${TagKey} (p. 717)		ec2:ResourceTag/ \${TagKey} (p. 721)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance (p. 696) aws:ResourceTag/ \${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:PlacementGroup (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)		
		internet- gateway (p. 697)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:InternetGatewayID (p. 719) ec2:ResourceTag/ \${TagKey} (p. 721)		
		local- gateway (p. 700)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		
		natgateway (p. 701)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-interface (p. 703)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:AssociatePublicIpAddress (p. 717) ec2:AuthorizedService (p. 717) ec2:AvailabilityZone (p. 718) ec2:NetworkInterfaceID (p. 719) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:Subnet (p. 721) ec2:Vpc (p. 722)	
			prefix-list (p. 704)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)	
			transit-gateway (p. 711)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)	
			vpc-endpoint (p. 713)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)	
			vpc-peering-connection (p. 714)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:AcceptorVpc (p. 717) ec2:RequesterVpc (p. 721) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:VpcPeeringConnectionID (p. 722)	
			vpn-gateway (p. 717)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)	
					ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ReplaceRouteTable	Grants permission to change the <code>route-table</code> that is associated with a subnet	Write	<code>route-table*</code> (p. 705) <code>aws:ResourceTag/\${TagKey}</code> (p. 717) <code>ec2:ResourceTag/\${TagKey}</code> (p. 721) <code>ec2:RouteTableID</code> (p. 721) <code>ec2:Vpc</code> (p. 722)		
			<code>subnet</code> (p. 709)	<code>aws:ResourceTag/\${TagKey}</code> (p. 717)	
				<code>ec2:AvailabilityZone</code> (p. 718)	
				<code>ec2:ResourceTag/\${TagKey}</code> (p. 721)	
				<code>ec2:SubnetID</code> (p. 722)	
				<code>ec2:Vpc</code> (p. 722)	
					<code>ec2:Region</code> (p. 720)
ReplaceTransitGatewayRouteTable	Grants permission to replace a <code>route-table</code> transit gateway route table	Write	<code>transit-gateway-route-table*</code> (p. 712) <code>aws:ResourceTag/\${TagKey}</code> (p. 721)	<code>ec2:ResourceTag/\${TagKey}</code> (p. 721)	
			<code>transit-gateway-attachment</code> (p. 710)	<code>aws:ResourceTag/\${TagKey}</code> (p. 717)	
				<code>ec2:ResourceTag/\${TagKey}</code> (p. 721)	
					<code>ec2:Region</code> (p. 720)
ReportInstanceState	Grants permission to submit feedback about the status of an instance	Write			<code>ec2:Region</code> (p. 720)
RequestSpotFleet	Grants permission to create a Spot Fleet request	Write	<code>spot-fleet-request*</code> (p. 708)	<code>aws:ResourceTag/\${TagKey}</code> (p. 717)	
				<code>ec2:ResourceTag/\${TagKey}</code> (p. 721)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			image (p. 694) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ImageID (p. 718) ec2:ImageType (p. 718) ec2:Owner (p. 719) ec2:Public (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RootDeviceType (p. 721)		
			key-pair (p. 699) aws:ResourceTag/ \${TagKey} (p. 717) ec2:KeyPairName (p. 719) ec2:KeyPairType (p. 719) ec2:ResourceTag/ \${TagKey} (p. 721)		
			launch-template (p. 699) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		
			placement-group (p. 703) aws:ResourceTag/ \${TagKey} (p. 717) ec2:PlacementGroupName (p. 720) ec2:PlacementGroupStrategy (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721)		
			security-group (p. 705) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SecurityGroupID (p. 721) ec2:Vpc (p. 722)		

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot (p. 207) aws:ResourceTag/ \${TagKey} (p. 717) ec2:OutpostArn (p. 719) ec2:Owner (p. 719) ec2:ParentVolume (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SnapshotID (p. 721) ec2:SnapshotTime (p. 721) ec2:SourceOutpostArn (p. 721) ec2:VolumeSize (p. 722)		
			subnet (p. 709) aws:ResourceTag/ \${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SubnetID (p. 722) ec2:Vpc (p. 722)		ec2:Region (p. 720)
RequestSpotInstances	Grants permission to create a Spot Instance request	Write	spot- instances- request* (p. 708)	aws:RequestTe aws>CreateTags aws:TagKey} (p. 717) aws:TagKeys (p. 717)	
			image (p. 694)	aws:ResourceTag/ \${TagKey} (p. 717)	
				ec2:ImageID (p. 718)	
				ec2:ImageType (p. 718)	
				ec2:Owner (p. 719)	
				ec2:Public (p. 720)	
				ec2:ResourceTag/ \${TagKey} (p. 721)	
				ec2:RootDeviceType (p. 721)	

Service Authorization Reference
 Service Authorization Reference
 Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			key-pair (p. 699)	aws:ResourceTag/\${TagKey} (p. 717) ec2:KeyPairName (p. 719) ec2:KeyPairType (p. 719) ec2:ResourceTag/\${TagKey} (p. 721)	
			network-interface (p. 703)	aws:ResourceTag/\${TagKey} (p. 717) ec2:AssociatePublicIpAddress (p. 717) ec2:AuthorizedService (p. 717) ec2:AuthorizedUser (p. 718) ec2:AvailabilityZone (p. 718) ec2:NetworkInterfaceID (p. 719) ec2:Permission (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Subnet (p. 721) ec2:Vpc (p. 722)	
			placement-group (p. 703)	aws:ResourceTag/\${TagKey} (p. 717) ec2:PlacementGroupName (p. 720) ec2:PlacementGroupStrategy (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)	
			security-group (p. 705)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721) ec2:SecurityGroupID (p. 721) ec2:Vpc (p. 722)	

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot (p. 207) aws:ResourceTag/ \${TagKey} (p. 717) ec2:OutpostArn (p. 719) ec2:Owner (p. 719) ec2:ParentVolume (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SnapshotID (p. 721) ec2:SnapshotTime (p. 721) ec2:SourceOutpostArn (p. 721) ec2:VolumeSize (p. 722)		
	subnet (p. 709) aws:ResourceTag/ \${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SubnetID (p. 722) ec2:Vpc (p. 722)				
				ec2:Region (p. 720)	
ResetAddressAttribute	Grants permission to reset the attribute of the specified IP address	Write	elastic- ip* (p. 687)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:AllocationId (p. 717) ec2:Attribute (p. 717) ec2:Attribute/ \${AttributeName} (p. 717) ec2:Domain (p. 718) ec2:PublicIpAddress (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721)	ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ResetEbsDefaultKey	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 (p. 720)	
ResetFpgaImageAttribute	Grants permission to reset an attribute of an Amazon FPGA Image (AFI) to its default value	Write	fpga-image* (p. 69) \${TagKey} (p. 717)	aws:ResourceTag/\${TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:Owner (p. 719) ec2:Public (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)	
	ec2:Region (p. 720)				
ResetImageAttribute	Grants permission to reset an attribute of an Amazon Machine Image (AMI) to its default value	Write	image* (p. 69) \${TagKey} (p. 717)	aws:ResourceTag/\${TagKey} (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:ImageID (p. 718) ec2:ImageType (p. 718) ec2:Owner (p. 719) ec2:Public (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RootDeviceType (p. 721)	ec2:Region (p. 720)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

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* (p. 695) ResourceTag/ \${TagKey} (p. 717)		ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:ProductCode (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)
	ec2:Region (p. 720)				
ResetNetworkInterfaceAttribute	Grants permission to reset an attribute of a network interface	Write	network- interface* (p. 701) ResourceTag/ \${TagKey} (p. 717)		aws:ResourceTag/ \${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:NetworkInterfaceID (p. 719) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:Subnet (p. 721) ec2:Vpc (p. 722)
	ec2:Region (p. 720)				

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ResetSnapshotAttribute	Grants permission to reset permissions settings for a snapshot	Permissions management	snapshot* (aws:ResourceTag/\${TagKey} (p. 717)) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:Owner (p. 719) ec2:ParentVolume (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:SnapshotID (p. 721) ec2:SnapshotTime (p. 721) ec2:VolumeSize (p. 722)		ec2:Region (p. 720)
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 (p. 720)
RestoreImageFromRecycleBin	Grants permission to restore an Amazon Machine Image (AMI) from the Recycle Bin	Write	image* (aws:ResourceTag/\${TagKey} (p. 717)) ec2:ImageID (p. 718) ec2:ImageType (p. 718) ec2:Owner (p. 719) ec2:Public (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RootDeviceType (p. 721)		ec2:Region (p. 720)
RestoreManagedPrefixListEntries	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* (p. 704) aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)		ec2:Region (p. 720)

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* (p. 705) ResourceTag/ {\$TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:Encrypted (p. 718) ec2:Owner (p. 719) ec2:ParentVolume (p. 720) ec2:ResourceTag/ {\$TagKey} (p. 721) ec2:SnapshotID (p. 721) ec2:SnapshotTime (p. 721) ec2:VolumeSize (p. 722)		ec2:Region (p. 720)
RestoreSnapshotTemporarily	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* (p. 705) ResourceTag/ {\$TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:Encrypted (p. 718) ec2:Owner (p. 719) ec2:ParentVolume (p. 720) ec2:ResourceTag/ {\$TagKey} (p. 721) ec2:SnapshotID (p. 721) ec2:SnapshotTime (p. 721) ec2:VolumeSize (p. 722)		ec2:Region (p. 720)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RevokeClientVpnInboundAuthorization	Grants permission to remove an inbound authorization rule from a Client VPN endpoint	Write	client-vpn-endpoint* (p. 718) aws:ResourceTag/\${TagKey} (p. 717)	aws:ResourceTag/ aws:ResourceTag/\${TagKey} (p. 717)	ec2:ClientRootCertificateChainArn (p. 718) ec2:CloudwatchLogGroupArn (p. 718) ec2:CloudwatchLogStreamArn (p. 718) ec2:DirectoryArn (p. 718) ec2:ResourceTag/ aws:ResourceTag/\${TagKey} (p. 721) ec2:SamlProviderArn (p. 721) ec2:ServerCertificateArn (p. 721)
RevokeSecurityGroupOutboundRules	Grants permission to remove one or more outbound rules from a VPC security group	Write	security-group* (p. 70) aws:ResourceTag/\${TagKey} (p. 717)	aws:ResourceTag/ aws:ResourceTag/\${TagKey} (p. 721)	ec2:ResourceTag/ aws:ResourceTag/\${TagKey} (p. 721) ec2:SecurityGroupID (p. 721) ec2:Vpc (p. 722)
RevokeSecurityGroupInboundRules	Grants permission to remove one or more inbound rules from a security group	Write	security-group* (p. 70) aws:ResourceTag/\${TagKey} (p. 717)	aws:ResourceTag/ aws:ResourceTag/\${TagKey} (p. 721)	ec2:ResourceTag/ aws:ResourceTag/\${TagKey} (p. 721) ec2:SecurityGroupID (p. 721) ec2:Vpc (p. 722)
					ec2:Region (p. 720)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RunInstances	Grants permission to launch one or more instances	Write	image* (p. 694) aws:ResourceTag/\${TagKey} (p. 717)		ec2:ImageID (p. 718) ec2:ImageType (p. 718) ec2:IsLaunchTemplateResource (p. 719) ec2:LaunchTemplate (p. 719) ec2:Owner (p. 719) ec2:Public (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RootDeviceType (p. 721)

Service Authorization Reference
 Service Authorization Reference
 Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance* (p. 695) RequestTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceAutoRecovery (p. 719) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceMetadataTags (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:IsLaunchTemplateResource (p. 719) ec2:LaunchTemplate (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:PlacementGroup (p. 720) ec2:ProductCode (p. 720) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)		

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-interface* (p. 70\$[TagKey} (p. 717)	aws:RequestTag/ aws:TagKeys (p. 717)	ec2:AssociatePublicIpAddress (p. 717) ec2:AuthorizedService (p. 717) ec2:AvailabilityZone (p. 718) ec2:IsLaunchTemplateResource (p. 719) ec2:LaunchTemplate (p. 719) ec2:NetworkInterfaceID (p. 719) ec2:Subnet (p. 721) ec2:Vpc (p. 722)
			security-group* (p. 70\$[TagKey} (p. 717)	aws:ResourceTag/ ec2:IsLaunchTemplateResource (p. 719)	ec2:LaunchTemplate (p. 719) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SecurityGroupID (p. 721) ec2:Vpc (p. 722)
			subnet* (p. 70\$[TagKey} (p. 717)	aws:ResourceTag/ \${TagKey} (p. 717)	ec2:AvailabilityZone (p. 718) ec2:IsLaunchTemplateResource (p. 719) ec2:LaunchTemplate (p. 719) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SubnetID (p. 722) ec2:Vpc (p. 722)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume* (p. 712) aws:RequestTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:AvailabilityZone (p. 718) ec2:Encrypted (p. 718) ec2:IsLaunchTemplateResource (p. 719) ec2:LaunchTemplate (p. 719) ec2:ParentSnapshot (p. 720) ec2:VolumeID (p. 722) ec2:VolumeProps (p. 722) ec2:VolumeSize (p. 722) ec2:VolumeThroughput (p. 722) ec2:VolumeType (p. 722)		
			capacity- reservation (p. 698) aws:ResourceTag/ \${TagKey} (p. 717) ec2:IsLaunchTemplateResource (p. 719) ec2:LaunchTemplate (p. 719) ec2:ResourceTag/ \${TagKey} (p. 721)		
			elastic- gpu (p. 691) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ElasticGpuType (p. 718) ec2:IsLaunchTemplateResource (p. 719) ec2:LaunchTemplate (p. 719) ec2:ResourceTag/ \${TagKey} (p. 721)		
			elastic- inference (p. 691)		
			group (p. 705)		

Service Authorization Reference
 Service Authorization Reference
 Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			key-pair (p. 699)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:IsLaunchTemplateResource (p. 719) ec2:KeyPairName (p. 719) ec2:KeyPairType (p. 719) ec2:LaunchTemplate (p. 719) ec2:ResourceTag/ \${TagKey} (p. 721)	
			launch-template (p. 703)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:IsLaunchTemplateResource (p. 719) ec2:LaunchTemplate (p. 719) ec2:ResourceTag/ \${TagKey} (p. 721)	
			license-configuration (p. 699)		
			placement-group (p. 703)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:IsLaunchTemplateResource (p. 719) ec2:LaunchTemplate (p. 719) ec2:PlacementGroupName (p. 720) ec2:PlacementGroupStrategy (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721)	

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot (p. 207) ec2:ResourceTag/ \${TagKey} (p. 717) ec2:IsLaunchTemplateResource (p. 719) ec2:LaunchTemplate (p. 719) ec2:Owner (p. 719) ec2:ParentVolume (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SnapshotID (p. 721) ec2:SnapshotTime (p. 721) ec2:VolumeSize (p. 722)		ec2:Region (p. 720)
	SCENARIO: EC2-Classic-EBS		image* (p. 694) instance* (p. 696) security- group* (p. 705) volume* (p. 712) key- pair (p. 699) placement- group (p. 703) snapshot (p. 707)		
	SCENARIO: EC2-Classic- InstanceStore		image* (p. 694) instance* (p. 696) security- group* (p. 705) key- pair (p. 699) placement- group (p. 703) snapshot (p. 707)		

Service Authorization Reference
 Service Authorization Reference
 Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	SCENARIO: EC2-VPC-EBS		image* (p. 694) instance* (p. 696) network-interface* (p. 703) security-group* (p. 705) volume* (p. 712) key-pair (p. 699) placement-group (p. 703) snapshot (p. 707)		
	SCENARIO: EC2-VPC-EBS-Subnet		image* (p. 694) instance* (p. 696) network-interface* (p. 703) security-group* (p. 705) subnet* (p. 709) volume* (p. 712) key-pair (p. 699) placement-group (p. 703) snapshot (p. 707)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	SCENARIO: EC2-VPC-InstanceStore		image* (p. 694) instance* (p. 696) network-interface* (p. 703) security-group* (p. 705) key-pair (p. 699) placement-group (p. 703) snapshot (p. 707)		
	SCENARIO: EC2-VPC-InstanceStore-Subnet		image* (p. 694) instance* (p. 696) network-interface* (p. 703) security-group* (p. 705) subnet* (p. 709) key-pair (p. 699) placement-group (p. 703) snapshot (p. 707)		
RunScheduledInstances	Grants permission to launch one or more Scheduled Instances	Write	image* (p. 694) aws:ResourceTag/\${TagKey} (p. 717) ec2:ImageID (p. 718) ec2:ImageType (p. 718) ec2:Owner (p. 719) ec2:Public (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RootDeviceType (p. 721)		

Service Authorization Reference
 Service Authorization Reference
 Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			key-pair (p. 699)	aws:ResourceTag/\${TagKey} (p. 717) ec2:KeyPairName (p. 719) ec2:KeyPairType (p. 719) ec2:ResourceTag/\${TagKey} (p. 721)	
			network-interface (p. 703)	aws:ResourceTag/\${TagKey} (p. 717) ec2:AssociatePublicIpAddress (p. 717) ec2:AuthorizedService (p. 717) ec2:AvailabilityZone (p. 718) ec2:NetworkInterfaceID (p. 719) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Subnet (p. 721) ec2:Vpc (p. 722)	
			placement-group (p. 703)	aws:ResourceTag/\${TagKey} (p. 717) ec2:PlacementGroupName (p. 720) ec2:PlacementGroupStrategy (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)	
			security-group (p. 705)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721) ec2:SecurityGroupID (p. 721) ec2:Vpc (p. 722)	

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot (p. 207) aws:ResourceTag/ \${TagKey} (p. 717) ec2:Owner (p. 719) ec2:ParentVolume (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SnapshotID (p. 721) ec2:SnapshotTime (p. 721) ec2:VolumeSize (p. 722)		
	subnet (p. 708) aws:ResourceTag/ \${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SubnetID (p. 722) ec2:Vpc (p. 722)				
				ec2:Region (p. 720)	
SearchLocalGatewayRoutes	Grants permission to search for local gateway route table	List			ec2:Region (p. 720)
SearchTransitGatewayGroups	Grants permission to search for groups, sources, and members in a transit gateway multicast domain	List			ec2:Region (p. 720)
SearchTransitGatewayRouteTables	Grants permission to search for route tables in a transit gateway route table	List	transit-gateway-route-table* (p. 712) aws:ResourceTag/ \${TagKey} (p. 717) ec2:ResourceTag/ \${TagKey} (p. 721)		ec2:Region (p. 720)

Service Authorization Reference
 Service Authorization Reference
 Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendDiagnosticInterrupt	Grants permission to send diagnostic interrupt to an Amazon EC2 instance	Write	instance* (p. 695) ResourceTag/\${TagKey} (p. 717)	ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceAutoRecovery (p. 719) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceMetadataTags (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)	ec2:Region (p. 720)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendSpotInstancePermission [permission only]	Grants permission to interrupt a Spot instance	Write	instance* (p. 696) ResourceTag/\${TagKey} (p. 717)	ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceAutoRecovery (p. 719) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceMetadataTags (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)	ec2:Region (p. 720)
StartInstances	Grants permission to start a stopped instance	Write	instance* (p. 696) ResourceTag/\${TagKey} (p. 717)	ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:PlacementGroup (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			license-configuration (p. 699)		
			ec2:Region (p. 720)		
StartNetworkInsightAnalysis	Grants permission to start a Network Access Scope analysis	Write	network-insights-access-scope-analysis* (p. 702)	aws:RequestTag/*CreateTags \${TagKey} (p. 717) aws:TagKeys (p. 717)	aws:RequestTag/*CreateTags \${TagKey} (p. 717)
	Grants permission to start analyzing a specified path	Write	network-insights-analysis* (p. 702)	ec2:ResourceTag/\${TagKey} (p. 721)	aws:RequestTag/*CreateTags \${TagKey} (p. 717)
			network-insights-path* (p. 702)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	aws:RequestTag/*CreateTags \${TagKey} (p. 717)
				ec2:Region (p. 720)	aws:RequestTag/*CreateTags \${TagKey} (p. 717)
StartVpcEndpointPrivateDnsVerification	Grants permission to start the Private DNS verification process for a VPC endpoint service	Write	vpc-endpoint-service* (p. 713)	aws:ResourceTag/\${TagKey} (p. 717) ec2:ResourceTag/\${TagKey} (p. 721)	aws:ResourceTag/\${TagKey} (p. 717)
				ec2:Region (p. 720)	ec2:Region (p. 720)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopInstances	Grants permission to stop an Amazon EBS-backed instance	Write	instance* (p. 695) ResourceTag/ \${TagKey} (p. 717)	ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:PlacementGroup (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)	ec2:Region (p. 720)
TerminateClientVpnConnections	Grants permission to terminate active Client VPN endpoint connections	Write	client-vpn- endpoint* (p. 689) ResourceTag/ \${TagKey} (p. 717)	aws:ResourceTag/ \${TagKey} (p. 717) ec2:ClientRootCertificateChainArn (p. 718) ec2:CloudwatchLogGroupArn (p. 718) ec2:CloudwatchLogStreamArn (p. 718) ec2:DirectoryArn (p. 718) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SamlProviderArn (p. 721) ec2:ServerCertificateArn (p. 721)	ec2:Region (p. 720)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TerminateInstances	Grants permission to shut down one or more instances	Write	instance* (p. 695) aws:ResourceTag/ \${TagKey} (p. 717)		ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:PlacementGroup (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)
UnassignIpv6Address	Grants permission to unassign one or more IPv6 addresses from a network interface	Write	network-interface* (p. 701) aws:ResourceTag/ \${TagKey} (p. 717)		ec2:AvailabilityZone (p. 718) ec2:NetworkInterfaceID (p. 719) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:Subnet (p. 721) ec2:Vpc (p. 722)

Service Authorization Reference
Service Authorization Reference
Amazon EC2

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* (p. 705)	aws:ResourceTag/\${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:NetworkInterfaceID (p. 719) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Subnet (p. 721) ec2:Vpc (p. 722)	ec2:Region (p. 720)
UnmonitorInstances	Grants permission to disable detailed monitoring for a running instance	Write	instance* (p. 696)	aws:ResourceTag/\${TagKey} (p. 717) ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceAutoRecovery (p. 719) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceMetadataTags (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:PlacementGroup (p. 720) ec2:ProductCode (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)	ec2:Region (p. 720)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateSecurityGroupIngress	Grants permission to update description for one or more outbound rules in a VPC security group	Write	security-group* (p. 70) [TagKey] (p. 717)	aws:ResourceTag/ ec2:ResourceTag/ \${TagKey} (p. 721)	ec2:SecurityGroupID (p. 721) ec2:Vpc (p. 722)
				ec2:Region (p. 720)	
UpdateSecurityGroupEgress	Grants permission to update description for one or more inbound rules in a security group	Write	security-group* (p. 70) [TagKey] (p. 717)	aws:ResourceTag/ ec2:ResourceTag/ \${TagKey} (p. 721)	ec2:SecurityGroupID (p. 721) ec2:Vpc (p. 722)
				ec2:Region (p. 720)	
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 (p. 720)

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 \(p. 501\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 717) aws:ResourceTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:AllocationId (p. 717) ec2:Attribute (p. 717)

Resource types	ARN	Condition keys
		ec2:Attribute/ \${AttributeName} (p. 717) ec2:Domain (p. 718) ec2:PublicIpAddress (p. 720) ec2:Region (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721)
capacity-reservation-fleet	<code>arn:\${Partition}:ec2:\${Region}: \${Account}:capacity-reservation-fleet/ \${CapacityReservationFleetId}</code>	aws:RequestTag/ \${TagKey} (p. 717) aws:ResourceTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Attribute (p. 717) ec2:Attribute/ \${AttributeName} (p. 717) ec2:Region (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721)
capacity-reservation	<code>arn:\${Partition}:ec2:\${Region}: \${Account}:capacity-reservation/ \${CapacityReservationId}</code>	aws:RequestTag/ \${TagKey} (p. 717) aws:ResourceTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Attribute (p. 717) ec2:Attribute/ \${AttributeName} (p. 717) ec2:CapacityReservationFleet (p. 718) ec2:IsLaunchTemplateResource (p. 719) ec2:LaunchTemplate (p. 719) ec2:Region (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721)

Resource types	ARN	Condition keys
carrier-gateway	<code>arn:\${Partition}:ec2:\${Region}: \${Account}:carrier-gateway/ \${CarrierGatewayId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Tenancy (p. 722) ec2:Vpc (p. 722)
certificate	<code>arn:\${Partition}:acm:\${Region}: \${Account}:certificate/\${CertificateId}</code>	
client-vpn-endpoint	<code>arn:\${Partition}:ec2:\${Region}: \${Account}:client-vpn-endpoint/ \${ClientVpnEndpointId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:ClientRootCertificateChainArn (p. 718) ec2:CloudwatchLogGroupArn (p. 718) ec2:CloudwatchLogStreamArn (p. 718) ec2:DirectoryArn (p. 718) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:SamlProviderArn (p. 721) ec2:ServerCertificateArn (p. 721)

Resource types	ARN	Condition keys
customer-gateway	<code>arn:\${Partition}:ec2:\${Region}: \${Account}:customer-gateway/ \${CustomerGatewayId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
dedicated-host	<code>arn:\${Partition}:ec2:\${Region}: \${Account}:dedicated-host/\${DedicatedHostId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:AutoPlacement (p. 718) ec2:AvailabilityZone (p. 718) ec2:HostRecovery (p. 718) ec2:InstanceType (p. 719) ec2:isLaunchTemplateResource (p. 719) ec2:LaunchTemplate (p. 719) ec2:Quantity (p. 720) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)

Resource types	ARN	Condition keys
dhcp-options	<code>arn:\${Partition}:ec2:\${Region}: \${Account}:dhcp-options/\${DhcpOptionsId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:DhcpOptionsID (p. 718) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
egress-only-internet-gateway	<code>arn:\${Partition}:ec2:\${Region}: \${Account}:egress-only-internet-gateway/ \${EgressOnlyInternetGatewayId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
elastic-gpu	<code>arn:\${Partition}:ec2:\${Region}: \${Account}:elastic-gpu/\${ElasticGpuId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:ElasticGpuType (p. 718) ec2:IsLaunchTemplateResource (p. 719) ec2:LaunchTemplate (p. 719) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
elastic-inference	<code>arn:\${Partition}:elastic-inference: \${Region}: \${Account}:elastic-inference-accelerator/\${ElasticInferenceAcceleratorId}</code>	

Resource types	ARN	Condition keys
export-image-task	<code>arn:\${Partition}:ec2:\${Region}:\${Account}:export-image-task/\${ExportImageTaskId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
export-instance-task	<code>arn:\${Partition}:ec2:\${Region}:\${Account}:export-instance-task/\${ExportTaskId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
fleet	<code>arn:\${Partition}:ec2:\${Region}:\${Account}:fleet/\${FleetId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)

Resource types	ARN	Condition keys
fpga-image	<code>arn:\${Partition}:ec2:\${Region}::fpga-image/\${FpgaImageId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:Owner (p. 719) ec2:Public (p. 720) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
host-reservation	<code>arn:\${Partition}:ec2:\${Region}:\${Account}:host-reservation/\${HostReservationId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)

Resource types	ARN	Condition keys
image	<code>arn:\${Partition}:ec2:\${Region}::image/\${ImageId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:ImageID (p. 718) ec2:ImageType (p. 718) ec2:IsLaunchTemplateResource (p. 719) ec2:LaunchTemplate (p. 719) ec2:Owner (p. 719) ec2:Public (p. 720) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RootDeviceType (p. 721)
import-image-task	<code>arn:\${Partition}:ec2:\${Region}:\${Account}:import-image-task/\${ImportImageTaskId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
import-snapshot-task	<code>arn:\${Partition}:ec2:\${Region}:\${Account}:import-snapshot-task/\${ImportSnapshotTaskId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)

Resource types	ARN	Condition keys
instance-event-window	<code>arn:\${Partition}:ec2:\${Region}:\${Account}:instance-event-window/\${InstanceEventWindowId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)

Resource types	ARN	Condition keys
instance	<code>arn:\${Partition}:ec2:\${Region}:\${Account}:instance/\${InstanceId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:AvailabilityZone (p. 718) ec2:EbsOptimized (p. 718) ec2:InstanceAutoRecovery (p. 719) ec2:InstanceId (p. 719) ec2:InstanceMarketType (p. 719) ec2:InstanceMetadataTags (p. 719) ec2:InstanceProfile (p. 719) ec2:InstanceType (p. 719) ec2:IsLaunchTemplateResource (p. 719) ec2:LaunchTemplate (p. 719) ec2:MetadataHttpEndpoint (p. 719) ec2:MetadataHttpPutResponseHopLimit (p. 719) ec2:MetadataHttpTokens (p. 719) ec2:NewInstanceProfile (p. 719) ec2:PlacementGroup (p. 720) ec2:ProductCode (p. 720) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RootDeviceType (p. 721) ec2:Tenancy (p. 722)

Resource types	ARN	Condition keys
internet-gateway	<code>arn:\${Partition}:ec2:\${Region}:\${Account}:internet-gateway/\${InternetGatewayId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:InternetGatewayID (p. 719) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
ipam	<code>arn:\${Partition}:ec2::\${Account}:ipam/\${IpamId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
ipam-pool	<code>arn:\${Partition}:ec2::\${Account}:ipam-pool/\${IpamPoolId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)

Resource types	ARN	Condition keys
ipam-scope	<code>arn:\${Partition}:ec2:\${Account}:ipam-scope/\${IpamScopeId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
ipv4pool-ec2	<code>arn:\${Partition}:ec2:\${Region}:\${Account}:ipv4pool-ec2/\${Ipv4PoolEc2Id}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
ipv6pool-ec2	<code>arn:\${Partition}:ec2:\${Region}:\${Account}:ipv6pool-ec2/\${Ipv6PoolEc2Id}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)

Resource types	ARN	Condition keys
key-pair	<code>arn:\${Partition}:ec2:\${Region}:\${Account}:key-pair/\${KeyPairName}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:IsLaunchTemplateResource (p. 719) ec2:KeyPairName (p. 719) ec2:KeyPairType (p. 719) ec2:LaunchTemplate (p. 719) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
launch-template	<code>arn:\${Partition}:ec2:\${Region}:\${Account}:launch-template/\${LaunchTemplateId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:IsLaunchTemplateResource (p. 719) ec2:LaunchTemplate (p. 719) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
license-configuration	<code>arn:\${Partition}:license-manager:\${Region}:\${Account}:license-configuration/\${LicenseConfigurationId}</code>	

Resource types	ARN	Condition keys
local-gateway	<code>arn:\${Partition}:ec2:\${Region}: \${Account}:local-gateway/\${LocalGatewayId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
local-gateway-route-table-virtual-interface-group-association	<code>arn:\${Partition}:ec2:\${Region}: \${Account}:local-gateway-route-table-virtual-interface-group-association/ \${LocalGatewayRouteTableVirtualInterfaceGroupAssociationId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
local-gateway-route-table-vpc-association	<code>arn:\${Partition}:ec2:\${Region}: \${Account}:local-gateway-route-table-vpc-association/ \${LocalGatewayRouteTableVpcAssociationId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
local-gateway-route-table	<code>arn:\${Partition}:ec2:\${Region}: \${Account}:local-gateway-route-table/ \${LocalGatewayRoutetableId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)

Resource types	ARN	Condition keys
local-gateway-virtual-interface-group	<code>arn:\${Partition}:ec2:\${Region}: \${Account}:local-gateway-virtual-interface-group/\${LocalGatewayVirtualInterfaceGroupId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
local-gateway-virtual-interface	<code>arn:\${Partition}:ec2:\${Region}: \${Account}:local-gateway-virtual-interface/ \${LocalGatewayVirtualInterfaceId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
natgateway	<code>arn:\${Partition}:ec2:\${Region}: \${Account}:natgateway/\${NatGatewayId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
network-acl	<code>arn:\${Partition}:ec2:\${Region}: \${Account}:network-acl/\${NaclId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:NetworkAclID (p. 719) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Vpc (p. 722)

Resource types	ARN	Condition keys
network-insights-access-scope-analysis	<code>arn:\${Partition}:ec2:\${Region}: \${Account}:network-insights-access-scope-analysis/ \${NetworkInsightsAccessScopeAnalysisId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
network-insights-access-scope	<code>arn:\${Partition}:ec2:\${Region}: \${Account}:network-insights-access-scope/ \${NetworkInsightsAccessScopeId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
network-insights-analysis	<code>arn:\${Partition}:ec2:\${Region}: \${Account}:network-insights-analysis/ \${NetworkInsightsAnalysisId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
network-insights-path	<code>arn:\${Partition}:ec2:\${Region}: \${Account}:network-insights-path/ \${NetworkInsightsPathId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)

Resource types	ARN	Condition keys
network-interface	<code>arn:\${Partition}:ec2:\${Region}:\${Account}:network-interface/\${NetworkInterfaceId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:AssociatePublicIpAddress (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:AuthorizedService (p. 717) ec2:AuthorizedUser (p. 718) ec2:AvailabilityZone (p. 718) ec2:IsLaunchTemplateResource (p. 719) ec2:LaunchTemplate (p. 719) ec2:NetworkInterfaceID (p. 719) ec2:Permission (p. 720) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Subnet (p. 721) ec2:Vpc (p. 722)
placement-group	<code>arn:\${Partition}:ec2:\${Region}:\${Account}:placement-group/\${PlacementGroupName}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:IsLaunchTemplateResource (p. 719) ec2:LaunchTemplate (p. 719) ec2:PlacementGroupName (p. 720) ec2:PlacementGroupStrategy (p. 720) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)

Resource types	ARN	Condition keys
prefix-list	<code>arn:\${Partition}:ec2:\${Region}:\${Account}:prefix-list/\${PrefixListId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
replace-root-volume-task	<code>arn:\${Partition}:ec2:\${Region}:\${Account}:replace-root-volume-task/\${ReplaceRootVolumeTaskId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
reserved-instances	<code>arn:\${Partition}:ec2:\${Region}:\${Account}:reserved-instances/\${ReservationId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:AvailabilityZone (p. 718) ec2:InstanceType (p. 719) ec2:Region (p. 720) ec2:ReservedInstancesOfferingType (p. 721) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Tenancy (p. 722)

Resource types	ARN	Condition keys
group	arn:\${Partition}:resource-groups:\${Region}: \${Account}:group/\${GroupName}	
role	arn:\${Partition}:iam::\${Account}:role/ \${RoleNameWithPath}	
route-table	arn:\${Partition}:ec2:\${Region}: \${Account}:route-table/\${RouteTableId}	aws:RequestTag/ \${TagKey} (p. 717) aws:ResourceTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:RouteTableID (p. 721) ec2:Vpc (p. 722)
security-group	arn:\${Partition}:ec2:\${Region}: \${Account}:security-group/\${SecurityGroupId}	aws:RequestTag/ \${TagKey} (p. 717) aws:ResourceTag/ \${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Attribute (p. 717) ec2:Attribute/ \${AttributeName} (p. 717) ec2:IsLaunchTemplateResource (p. 719) ec2:LaunchTemplate (p. 719) ec2:Region (p. 720) ec2:ResourceTag/ \${TagKey} (p. 721) ec2:SecurityGroupID (p. 721) ec2:Vpc (p. 722)

Resource types	ARN	Condition keys
security-group-rule	<code>arn:\${Partition}:ec2:\${Region}:\${Account}:security-group-rule/\${SecurityGroupRuleId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)

Resource types	ARN	Condition keys
snapshot	<code>arn:\${Partition}:ec2:\${Region}::snapshot/\${SnapshotId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Add/group (p. 717) ec2:Add/userId (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:AvailabilityZone (p. 718) ec2:Encrypted (p. 718) ec2:IsLaunchTemplateResource (p. 719) ec2:LaunchTemplate (p. 719) ec2:OutpostArn (p. 719) ec2:Owner (p. 719) ec2:ParentVolume (p. 720) ec2:Region (p. 720) ec2:Remove/group (p. 721) ec2:Remove/userId (p. 721) ec2:ResourceTag/\${TagKey} (p. 721) ec2:SnapshotID (p. 721) ec2:SnapshotTime (p. 721) ec2:SourceOutpostArn (p. 721) ec2:VolumeSize (p. 722)

Resource types	ARN	Condition keys
spot-fleet-request	arn:\${Partition}:ec2:\${Region}:\${Account}:spot-fleet-request/\${SpotFleetRequestId}	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
spot-instances-request	arn:\${Partition}:ec2:\${Region}:\${Account}:spot-instances-request/\${SpotInstanceRequestId}	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
subnet-cidr-reservation	arn:\${Partition}:ec2:\${Region}:\${Account}:subnet-cidr-reservation/\${SubnetCidrReservationId}	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)

Resource types	ARN	Condition keys
subnet	<code>arn:\${Partition}:ec2:\${Region}: \${Account}:subnet/\${SubnetId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:AvailabilityZone (p. 718) ec2:IsLaunchTemplateResource (p. 719) ec2:LaunchTemplate (p. 719) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:SubnetID (p. 722) ec2:Vpc (p. 722)
traffic-mirror-filter	<code>arn:\${Partition}:ec2:\${Region}: \${Account}:traffic-mirror-filter/ \${TrafficMirrorFilterId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
traffic-mirror-filter-rule	<code>arn:\${Partition}:ec2:\${Region}: \${Account}:traffic-mirror-filter-rule/ \${TrafficMirrorFilterRuleId}</code>	ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:Region (p. 720)

Resource types	ARN	Condition keys
traffic-mirror-session	arn:\${Partition}:ec2:\${Region}:\${Account}:traffic-mirror-session/\${TrafficMirrorSessionId}	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
traffic-mirror-target	arn:\${Partition}:ec2:\${Region}:\${Account}:traffic-mirror-target/\${TrafficMirrorTargetId}	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
transit-gateway-attachment	arn:\${Partition}:ec2:\${Region}:\${Account}:transit-gateway-attachment/\${TransitGatewayAttachmentId}	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)

Resource types	ARN	Condition keys
transit-gateway-connect-peer	<code>arn:\${Partition}:ec2:\${Region}:\${Account}:transit-gateway-connect-peer/\${TransitGatewayConnectPeerId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
transit-gateway	<code>arn:\${Partition}:ec2:\${Region}:\${Account}:transit-gateway/\${TransitGatewayId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
transit-gateway-multicast-domain	<code>arn:\${Partition}:ec2:\${Region}:\${Account}:transit-gateway-multicast-domain/\${TransitGatewayMulticastDomainId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)

Resource types	ARN	Condition keys
transit-gateway-route-table	<code>arn:\${Partition}:ec2:\${Region}:\${Account}:transit-gateway-route-table/\${TransitGatewayRouteTableId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)
volume	<code>arn:\${Partition}:ec2:\${Region}:\${Account}:volume/\${VolumeId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:AvailabilityZone (p. 718) ec2:Encrypted (p. 718) ec2:IsLaunchTemplateResource (p. 719) ec2:KmsKeyId (p. 719) ec2:LaunchTemplate (p. 719) ec2:ParentSnapshot (p. 720) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:VolumeID (p. 722) ec2:VolumeIops (p. 722) ec2:VolumeSize (p. 722) ec2:VolumeThroughput (p. 722) ec2:VolumeType (p. 722)

Resource types	ARN	Condition keys
vpc-endpoint	arn:\${Partition}:ec2:\${Region}: \${Account}:vpc-endpoint/\${VpcEndpointId}	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:VpceServiceName (p. 722) ec2:VpceServiceOwner (p. 722)
vpc-endpoint-service	arn:\${Partition}:ec2:\${Region}: \${Account}:vpc-endpoint-service/ \${VpcEndpointServiceId}	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:VpceServicePrivateDnsName (p. 722)
vpc-flow-log	arn:\${Partition}:ec2:\${Region}: \${Account}:vpc-flow-log/\${VpcFlowLogId}	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)

Resource types	ARN	Condition keys
vpc	arn:\${Partition}:ec2:\${Region}:\${Account}:vpc/\${VpcId}	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:Ipv4IpamPoolId (p. 719) ec2:Ipv6IpamPoolId (p. 719) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721) ec2:Tenancy (p. 722) ec2:VpcID (p. 722)
vpc-peering-connection	arn:\${Partition}:ec2:\${Region}:\${Account}:vpc-peering-connection/\${VpcPeeringConnectionId}	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:AcceptorVpc (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:Region (p. 720) ec2:RequesterVpc (p. 721) ec2:ResourceTag/\${TagKey} (p. 721) ec2:VpcPeeringConnectionID (p. 722)

Resource types	ARN	Condition keys
vpn-connection-device-type	<code>arn:\${Partition}:ec2:\${Region}:\${Account}:vpn-connection-device-type/\${VpnConnectionDeviceTypeId}</code>	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)

Resource types	ARN	Condition keys
vpn-connection	arn:\${Partition}:ec2:\${Region}:\${Account}:vpn-connection/\${VpnConnectionId}	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Attribute (p. 717) ec2:Attribute/\${AttributeName} (p. 717) ec2:AuthenticationType (p. 717) ec2:DPDTTimeoutSeconds (p. 718) ec2:GatewayType (p. 718) ec2:IKEVersions (p. 718) ec2:InsideTunnelCidr (p. 718) ec2:InsideTunnelIpv6Cidr (p. 718) ec2:Phase1DHGroup (p. 720) ec2:Phase1EncryptionAlgorithms (p. 720) ec2:Phase1IntegrityAlgorithms (p. 720) ec2:Phase1LifetimeSeconds (p. 720) ec2:Phase2DHGroup (p. 720) ec2:Phase2EncryptionAlgorithms (p. 720) ec2:Phase2IntegrityAlgorithms (p. 720) ec2:Phase2LifetimeSeconds (p. 720) ec2:PreSharedKeys (p. 720) ec2:Region (p. 720) ec2:RekeyFuzzPercentage (p. 721) ec2:RekeyMarginTimeSeconds (p. 721) ec2:ReplayWindowSizePackets (p. 721) ec2:ResourceTag/\${TagKey} (p. 721) ec2:RoutingType (p. 721)

Resource types	ARN	Condition keys
vpn-gateway	arn:\${Partition}:ec2:\${Region}:\${Account}:vpn-gateway/\${VpnGatewayId}	aws:RequestTag/\${TagKey} (p. 717) aws:ResourceTag/\${TagKey} (p. 717) aws:TagKeys (p. 717) ec2:Region (p. 720) ec2:ResourceTag/\${TagKey} (p. 721)

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 [Available global condition 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:AcceptorVpc	Filters access by the ARN of an accepter VPC in a VPC peering connection	ARN
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

Condition keys	Description	Type
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: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>CreateAction	Filters access by the name of a resource-creating API action	String
ec2:DPDTimeoutSeconds	Filters access by the duration after which DPD timeout occurs on a VPN tunnel	Numeric
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: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	String
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:InsideTunnelIpv6	Filters access by a range of inside IPv6 addresses for a VPN tunnel	String

Condition keys	Description	Type
ec2:InstanceAutoRecovery	Filters access by whether the instance type supports auto-recovery	String
ec2:InstanceId	Filters access by the ID of an instance	String
ec2:InstanceMarketType	Filters access by the market or purchasing option of an instance (on-demand or spot)	String
ec2:InstanceMetadataTags	Filters access by whether the instance allows access to instance tags from the instance metadata	String
ec2:InstanceProfile	Filters access by the ARN of an instance profile	ARN
ec2:InstanceType	Filters access by the type of instance	String
ec2:InternetGatewayID	Filters access by the ID of an internet gateway	String
ec2:Ipv4IpamPoolId	Filters access by the ID of an IPAM pool provided for IPv4 CIDR block allocation	String
ec2:Ipv6IpamPoolId	Filters access by the ID of an IPAM pool provided for IPv6 CIDR block allocation	String
ec2:IsLaunchTemplateOverridesSpecified	Filters access by whether users are able to override resources specified in the launch template	Bool
ec2:KeyPairName	Filters access by the name of a key pair	String
ec2:KeyPairType	Filters access by the type of a key pair	String
ec2:KmsKeyId	Filters access by the ID of an AWS KMS key	String
ec2:LaunchTemplate	Filters access by the ARN of a launch template	ARN
ec2:MetadataHttpEnabled	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:MetadataHttpTo(instance)	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:NewInstanceProfileAttached	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	Numeric
ec2:Phase1EncryptionAlgorithm	Filters access by the encryption algorithms that are permitted for a VPN tunnel for the phase 1 IKE negotiations	String
ec2:Phase1IntegrityAlgorithm	Filters access by the integrity algorithms that are permitted for a VPN tunnel for the phase 1 IKE negotiations	String
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	Numeric
ec2:Phase2EncryptionAlgorithm	Filters access by the encryption algorithms that are permitted for a VPN tunnel for the phase 2 IKE negotiations	String
ec2:Phase2IntegrityAlgorithm	Filters access by the integrity algorithms that are permitted for a VPN tunnel for the phase 2 IKE negotiations	String
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:PreSharedKeys	Filters access by the pre-shared key (PSK) used to establish the initial IKE security association between a virtual private gateway and a customer gateway	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

Condition keys	Description	Type
ec2:RekeyFuzzPercent	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:RekeyMarginTime	Filters access by the margin time before the phase 2 lifetime expires for a VPN tunnel	Numeric
ec2:Remove/group	Filters access by the group being removed from a snapshot	String
ec2:Remove/userId	Filters access by the account id being removed from a snapshot	String
ec2:ReplayWindowSize	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/	Filters access by the preface string for a tag key and value pair that are attached to a resource	String
ec2:ResourceTag/\${TagKey}	Filters access by a tag key and value pair of a resource	String
ec2:RoleDelivery	Filters access by the version of the instance metadata service for retrieving IAM role credentials for EC2	Numeric
ec2:RootDeviceType	Filters access by the root device type of the instance (ebs or instance-store)	String
ec2:RouteTableID	Filters access by the ID of a route table	String
ec2:RoutingType	Filters access by the routing type for the VPN connection	String
ec2:SamlProviderArn	Filters access by the ARN of the IAM SAML identity provider	ARN
ec2:SecurityGroupID	Filters access by the ID of a security group	String
ec2:ServerCertificateArn	Filters access by the ARN of the server certificate	ARN
ec2:SnapshotID	Filters access by the ID of a snapshot	String
ec2:SnapshotTime	Filters access by the initiation time of a snapshot	String
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

Condition keys	Description	Type
ec2:SubnetID	Filters access by the ID of a subnet	String
ec2:Tenancy	Filters access by the tenancy of the VPC or instance (default, dedicated, or host)	String
ec2:VolumeID	Filters access by the ID of a volume	String
ec2:VolumeIOPS	Filters access by the the number of input/output operations per second (IOPS) provisioned for the volume	Numeric
ec2:VolumeSize	Filters access by the size of the volume, in GiB	Numeric
ec2:VolumeThroughput	Filters access by the throughput of the volume, in MiBps	Numeric
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:VpcServiceName	Filters access by the name of the VPC endpoint service	String
ec2:VpcServiceOwnerService	Filters access by the service owner of the VPC endpoint service (amazon, aws-marketplace, or an AWS account ID)	String
ec2:VpcServicePrivateServiceName	Filters access by the private DNS name of the VPC endpoint	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 \(p. 723\)](#)
- [Resource types defined by Amazon EC2 Auto Scaling \(p. 730\)](#)
- [Condition keys for Amazon EC2 Auto Scaling \(p. 731\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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	autoScaling:GroupARNs (p. 731) aws:ResourceTag/\${TagKey} (p. 731) aws:ResourceTag/\${TagKey} (p. 732)		
AttachLoadBalancerTargetGroups	Grants permission to attach one or more target groups to the specified Auto Scaling group	Write	autoScaling:GroupARNs (p. 731) aws:ResourceTag/\${TagKey} (p. 731) aws:ResourceTag/\${TagKey} (p. 732)		autoscaling:TargetGroupARNs (p. 731)
					autoscaling:LoadBalancerNames (p. 731)
AttachLoadBalancers	Grants permission to attach one or more load balancers to the specified Auto Scaling group	Write	autoScaling:GroupARNs (p. 731) aws:ResourceTag/\${TagKey} (p. 731) aws:ResourceTag/\${TagKey} (p. 732)		
					autoscaling:LoadBalancerNames (p. 731)
BatchDeleteScheduledActions	Grants permission to delete the specified scheduled actions	Write	autoScaling:GroupARNs (p. 731) aws:ResourceTag/\${TagKey} (p. 731) aws:ResourceTag/\${TagKey} (p. 732)		
BatchPutScheduledActions	Grants permission to create or update multiple scheduled scaling actions for an Auto Scaling group	Write	autoScaling:GroupARNs (p. 731) aws:ResourceTag/\${TagKey} (p. 731) aws:ResourceTag/\${TagKey} (p. 732)		
CancelInstanceRefresh	Grants permission to cancel an instance refresh operation in progress	Write	autoScaling:GroupARNs (p. 731) aws:ResourceTag/\${TagKey} (p. 731)		

Service Authorization Reference
Service Authorization Reference
Amazon EC2 Auto Scaling

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					aws:ResourceTag/ \${TagKey} (p. 732)
CompleteLifecycleToken	Grants permission to complete the lifecycle action for the specified token or instance with the specified result	Write	autoScaling:GroupARN autoScaling:ResourceTag/ \${TagKey} (p. 731)		aws:ResourceTag/ \${TagKey} (p. 732)
CreateAutoScalingGroup	Grants permission to create an Auto Scaling group with the specified name and attributes	Write	autoScaling:GroupARN autoScaling:ResourceTag/ \${TagKey} (p. 731)		aws:ResourceTag/ \${TagKey} (p. 732)
					autoscaling:InstanceTypes (p. 731) autoscaling:LaunchConfigurationName autoscaling:LaunchTemplateVersionSp autoscaling:LoadBalancerNames (p. 731) autoscaling:MaxSize (p. 731) autoscaling:MinSize (p. 731) autoscaling:TargetGroupARNs (p. 731) autoscaling:VPCZoneIdentifiers (p. 731) aws:RequestTag/ \${TagKey} (p. 731) aws:TagKeys (p. 732)
CreateLaunchConfiguration	Grants permission to create a launch configuration	Write	launchConfiguration* (p. 730)		
CreateOrUpdateTags	Grants permission to create or update tags for the specified Auto Scaling group	Tagging	autoScaling:GroupARN autoScaling:ResourceTag/ \${TagKey} (p. 731)		aws:ResourceTag/ \${TagKey} (p. 732)

Service Authorization Reference
Service Authorization Reference
Amazon EC2 Auto Scaling

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 731)	aws:TagKeys (p. 732)
DeleteAutoScalingGroup	Grants permission to delete the specified Auto Scaling group	Write	autoScaling	GroupScaling	ResourceTag/ \${TagKey} (p. 731)
DeleteLaunchConfiguration	Grants permission to delete the specified launch configuration	Write	launchConfiguration*	(p. 730)	
DeleteLifecycleHook	Grants permission to deletes the specified lifecycle hook	Write	autoScaling	GroupScaling	ResourceTag/ \${TagKey} (p. 731)
DeleteNotification	Grants permission to delete the specified notification	Write	autoScaling	GroupScaling	ResourceTag/ \${TagKey} (p. 731)
DeletePolicy	Grants permission to delete the specified Auto Scaling policy	Write	autoScaling	GroupScaling	ResourceTag/ \${TagKey} (p. 731)
DeleteScheduledAction	Grants permission to delete the specified scheduled action	Write	autoScaling	GroupScaling	ResourceTag/ \${TagKey} (p. 731)
DeleteTags	Grants permission to delete the specified tags	Tagging	autoScaling	GroupScaling	ResourceTag/ \${TagKey} (p. 731)
					aws:RequestTag/ \${TagKey} (p. 731)
DeleteWarmPool	Grants permission to delete the warm pool associated with the Auto Scaling group	Write	autoScaling	GroupScaling	ResourceTag/ \${TagKey} (p. 731)
					aws:ResourceTag/ \${TagKey} (p. 732)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeAccountLimits	Grants permission to describe the current Auto Scaling resource limits for your AWS account	List			
DescribeAdjustmentTypes	Grants permission to describe the policy adjustment types for use with PutScalingPolicy	List			
DescribeAutoScalingGroups	Grants permission to describe one or more Auto Scaling groups. If a list of names is not provided, the call describes all Auto Scaling groups	List			
DescribeAutoScalingInstances	Grants permission to describe one or more Auto Scaling instances. If a list is not provided, the call describes all instances	List			
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			
DescribeLifecycleHooks	Grants permission to describe the available types of lifecycle hooks	List			
DescribeLifecycleHooksForAutoScaling	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			
DescribeMetricCollectionMetrics	Grants permission to describe the available CloudWatch metrics for Auto Scaling	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeNotificationActions	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 more scaling activities for the specified Auto Scaling group	List			
DescribeScalingProcessTypes	Grants permission to describe the scaling process types for use with ResumeProcesses and SuspendProcesses	List			
DescribeScheduledActions	Grants permission to describe the actions scheduled for your Auto Scaling group that haven't run	List			
DescribeTags	Grants permission to describe the specified tags	Read			
DescribeTerminationPolicies	Grants permission to describe the termination policies supported by Auto Scaling	List			
DescribeWarmPool	Grants permission to describe the warm pool associated with the Auto Scaling group	List			
DetachInstances	Grants permission to remove one or more instances from the specified Auto Scaling group	Write	autoScaling:GroupARNs (p. 731) aws:ResourceTag/\${TagKey} (p. 731) aws:ResourceTag/\${TagKey} (p. 732)		
DetachLoadBalancers	Grants permission to detach one or more target groups from the specified Auto Scaling group	Write	autoScaling:GroupARNs (p. 731) aws:ResourceTag/\${TagKey} (p. 731) aws:ResourceTag/\${TagKey} (p. 732) autoscaling:TargetGroupARNs (p. 731)		
DetachLoadBalancers	Grants permission to remove one or more load balancers from the specified Auto Scaling group	Write	autoScaling:GroupARNs (p. 731) aws:ResourceTag/\${TagKey} (p. 731) aws:ResourceTag/\${TagKey} (p. 732) autoscaling:LoadBalancerNames (p. 731)		

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	autoScaling	GroupScalingResourceTag/\${TagKey} (p. 731) aws:ResourceTag/\${TagKey} (p. 732)	
EnableMetricsCollection	Grants permission to enable monitoring of the specified metrics for the specified Auto Scaling group	Write	autoScaling	GroupScalingResourceTag/\${TagKey} (p. 731) aws:ResourceTag/\${TagKey} (p. 732)	
EnterStandby	Grants permission to move the specified instances into Standby mode	Write	autoScaling	GroupScalingResourceTag/\${TagKey} (p. 731) aws:ResourceTag/\${TagKey} (p. 732)	
ExecutePolicy	Grants permission to execute the specified policy	Write	autoScaling	GroupScalingResourceTag/\${TagKey} (p. 731) aws:ResourceTag/\${TagKey} (p. 732)	
ExitStandby	Grants permission to move the specified instances out of Standby mode	Write	autoScaling	GroupScalingResourceTag/\${TagKey} (p. 731) aws:ResourceTag/\${TagKey} (p. 732)	
GetPredictiveScalingForecast	Grants permission to retrieve the Forecast data for a predictive scaling policy	List			
PutLifecycleHook	Grants permission to create or update a lifecycle hook for the specified Auto Scaling Group	Write	autoScaling	GroupScalingResourceTag/\${TagKey} (p. 731) aws:ResourceTag/\${TagKey} (p. 732)	
PutNotificationConfig	Grants permission to configure an Auto Scaling group to send notifications when specified events take place	Write	autoScaling	GroupScalingResourceTag/\${TagKey} (p. 731) aws:ResourceTag/\${TagKey} (p. 732)	
PutScalingPolicy	Grants permission to create or update a policy for an Auto Scaling group	Write	autoScaling	GroupScalingResourceTag/\${TagKey} (p. 731) aws:ResourceTag/\${TagKey} (p. 732)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutScheduledUpdateAction	Grants permission to create or update a scheduled scaling action for an Auto Scaling group	Write	autoScaling	GroupScaling ResourceTag/ \${TagKey} (p. 731) aws:ResourceTag/ \${TagKey} (p. 732)	PutScalingPolicy ResourceTag/ \${TagKey} (p. 731) autoscaling:MaxSize (p. 731) autoscaling:MinSize (p. 731)
PutWarmPool	Grants permission to create or update the warm pool associated with the specified Auto Scaling group	Write	autoScaling	GroupScaling ResourceTag/ \${TagKey} (p. 731) aws:ResourceTag/ \${TagKey} (p. 732)	PutScalingPolicy ResourceTag/ \${TagKey} (p. 731) ResourceTag/ \${TagKey} (p. 732)
RecordLifecycleActionResult	Grants permission to record a heartbeat for the lifecycle action associated with the specified token or instance	Write	autoScaling	GroupScaling ResourceTag/ \${TagKey} (p. 731) aws:ResourceTag/ \${TagKey} (p. 732)	PutScalingPolicy ResourceTag/ \${TagKey} (p. 731) ResourceTag/ \${TagKey} (p. 732)
ResumeProcesses	Grants permission to resume the specified suspended Auto Scaling processes, or all suspended process, for the specified Auto Scaling group	Write	autoScaling	GroupScaling ResourceTag/ \${TagKey} (p. 731) aws:ResourceTag/ \${TagKey} (p. 732)	PutScalingPolicy ResourceTag/ \${TagKey} (p. 731) ResourceTag/ \${TagKey} (p. 732)
SetDesiredCapacity	Grants permission to set the size of the specified Auto Scaling group	Write	autoScaling	GroupScaling ResourceTag/ \${TagKey} (p. 731) aws:ResourceTag/ \${TagKey} (p. 732)	PutScalingPolicy ResourceTag/ \${TagKey} (p. 731) ResourceTag/ \${TagKey} (p. 732)
SetInstanceHealth	Grants permission to set the health status of the specified instance	Write	autoScaling	GroupScaling ResourceTag/ \${TagKey} (p. 731) aws:ResourceTag/ \${TagKey} (p. 732)	PutScalingPolicy ResourceTag/ \${TagKey} (p. 731) ResourceTag/ \${TagKey} (p. 732)
SetInstanceProtection	Grants permission to update the instance protection settings of the specified instances	Write	autoScaling	GroupScaling ResourceTag/ \${TagKey} (p. 731) aws:ResourceTag/ \${TagKey} (p. 732)	PutScalingPolicy ResourceTag/ \${TagKey} (p. 731) ResourceTag/ \${TagKey} (p. 732)
StartInstanceRefresh	Grants permission to start a new instance refresh operation	Write	autoScaling	GroupScaling ResourceTag/ \${TagKey} (p. 731) aws:ResourceTag/ \${TagKey} (p. 732)	PutScalingPolicy ResourceTag/ \${TagKey} (p. 731) ResourceTag/ \${TagKey} (p. 732)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SuspendProcesses	Grants permission to suspend the specified Auto Scaling processes, or all processes, for the specified Auto Scaling group	Write	autoScaling	autoScaling:ResourceTag/ \${TagKey} (p. 731) aws:ResourceTag/ \${TagKey} (p. 732)	
TerminateInstances	Grants permission to terminate the specified instance and optionally adjust the desired group size	Write	autoScaling	autoScaling:ResourceTag/ \${TagKey} (p. 731) aws:ResourceTag/ \${TagKey} (p. 732)	
UpdateAutoScalingConfiguration	Grants permission to update the configuration for the specified Auto Scaling group	Write	autoScaling	autoScaling:ResourceTag/ \${TagKey} (p. 731) aws:ResourceTag/ \${TagKey} (p. 732)	autoscaling:InstanceTypes (p. 731) autoscaling:LaunchConfigurationName autoscaling:LaunchTemplateVersionSp autoscaling:MaxSize (p. 731) autoscaling:MinSize (p. 731) autoscaling:VPCZoneIdentifiers (p. 731)

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](#) (p. 723) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 731) aws:ResourceTag/ \${TagKey} (p. 732)
launchConfiguration	arn:\${Partition}:autoscaling:\${Region}:\${Account}:launchConfiguration:\${Id}:launchConfigurationName/\${LaunchConfigurationName}	

Condition keys for Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see [Condition keys table](#).

To view the global condition keys that are available to all services, see [Available global condition keys](#).

Condition keys	Description	Type
autoscaling:ImageId	Filters access based on the AMI used to create the instance	String
autoscaling:InstanceType	Filters access based on the type of instance, in terms of the hardware resources available	String
autoscaling:InstanceType	Filters access based on the types of instances, in terms of the hardware resources available	String
autoscaling:LaunchConfigurationName	Filters access based on the name of a launch configuration	String
autoscaling:LaunchTemplate	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	String
autoscaling:MaxSize	Filters access based on the maximum scaling size	Numeric
autoscaling:MetadataEndpoint	Filters access based on whether the HTTP endpoint is enabled for the instance metadata service	String
autoscaling:MetadataHops	Filters access based on the allowed number of hops when calling the instance metadata service	Numeric
autoscaling:MetadataTokens	Filters access based on whether tokens are required when calling the instance metadata service (optional or required)	String
autoscaling:MinSize	Filters access based on the minimum scaling size	Numeric
autoscaling:ResourceTag	Filters access based on the value of a tag attached to a resource	String
autoscaling:SpotPrice	Filters access based on the spot price associated with an instance	Numeric
autoscaling:TargetGroupARNs	Filters access based on the ARN of a target group	ARN
autoscaling:VPCZoneIdentifiers	Filters access based on the identifier of a VPC zone	String
aws:RequestTag/\${TagKey}	Filters access based on the value of a tag associated with the request	String

Condition keys	Description	Type
aws:ResourceTag/\${TagKey}	Filters access based on the tag-value associated with the resource	String
aws:TagKeys	Filters create requests based on the presence of mandatory tags in the request	String

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 \(p. 732\)](#)
- [Resource types defined by Amazon EC2 Image Builder \(p. 739\)](#)
- [Condition keys for Amazon EC2 Image Builder \(p. 740\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 739)		
CreateComponent	Grants permission to create a new component	Write	component* (p. 739)		iam>CreateServiceLinkedRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithCustomKeyMaterial kmsKey (p. 740) aws:RequestTag/\${TagKey} (p. 740) aws:TagKeys (p. 740)
CreateContainerRecipe	Grants permission to create a new Container Recipe	Write	containerRecipe* (p. 739)		ecr:DescribeImages ecr:DescribeRepositories iam:CreateServiceLinkedRole imagebuilder:GetComponent imagebuilder:GetImage imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithCustomKeyMaterial aws:RequestTag/\${TagKey} (p. 740) aws:TagKeys (p. 740)
CreateDistribution	Grants permission to create a new distribution configuration	Write	distributionConfiguration* (p. 739)	iam:CreateServiceLinkedRole imagebuilder:TagResource	
CreateImage	Grants permission to create a new image	Write	image* (p. 739)		iam:CreateServiceLinkedRole imagebuilder:GetContainer imagebuilder:GetDistribution imagebuilder:GetImageResult imagebuilder:GetInfrastructure imagebuilder:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 740) aws:TagKeys (p. 740)	
CreateImagePipeline	Grants permission to create a new image pipeline	Write	imagePipeline* (p. 740)	iam:CreateServiceLinkedRole imagebuilder:GetContainerDefinitions imagebuilder:GetImageRecipe imagebuilder:TagResource	iam:CreateServiceLinkedRole imagebuilder:GetContainerDefinitions imagebuilder:GetImageRecipe imagebuilder:TagResource
					aws:RequestTag/ \${TagKey} (p. 740) aws:TagKeys (p. 740)
CreateImageRecipe	Grants permission to create a new Image Recipe	Write	imageRecipe* (p. 739)	ec2:DescribeImages iam:CreateServiceLinkedRole imagebuilder:GetComponent imagebuilder:GetImage imagebuilder:TagResource	ec2:DescribeImages iam:CreateServiceLinkedRole imagebuilder:GetComponent imagebuilder:GetImage imagebuilder:TagResource
					aws:RequestTag/ \${TagKey} (p. 740) aws:TagKeys (p. 740)
CreateInfrastructureConfiguration	Grants permission to create a new infrastructure configuration	Write	infrastructureConfiguration* (p. 740)	iam:CreateServiceLinkedRole iam:PassRole imagebuilder:TagResource sns:Publish	iam:CreateServiceLinkedRole iam:PassRole imagebuilder:TagResource sns:Publish
					aws:RequestTag/ \${TagKey} (p. 740) aws:TagKeys (p. 740) imagebuilder:CreatedResourceTagKeys imagebuilder:CreatedResourceTag/ <key> (p. 740) imagebuilder:Ec2MetadataHttpTokens imagebuilder:StatusTopicArn (p. 740)
DeleteComponent	Grants permission to delete a component	Write	component* (p. 739)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteContainerRecipe	Grants permission to delete a container recipe	Write	containerRecipe* (p. 739)		
DeleteDistributionConfiguration	Grants permission to delete a distribution configuration	Write	distributionConfiguration* (p. 739)		
DeleteImage	Grants permission to delete an image	Write	image* (p. 739)		
DeleteImagePipeline	Grants permission to delete an image pipeline	Write	imagePipeline* (p. 740)		
DeleteImageRecipe	Grants permission to delete an image recipe	Write	imageRecipe* (p. 739)		
DeleteInfrastructureConfiguration	Grants permission to delete an infrastructure configuration	Write	infrastructureConfiguration* (p. 740)		
GetComponent	Grants permission to view details about a component	Read	component* (p. 739)	kms:Decrypt	
GetComponentPolicy	Grants permission to view the resource policy associated with a component	Read	component* (p. 739)		
GetContainerRecipe	Grants permission to view details about a container recipe	Read	containerRecipe* (p. 739)		
GetContainerRecipePolicy	Grants permission to view the resource policy associated with a container recipe	Read	containerRecipe* (p. 739)		
GetDistributionConfiguration	Grants permission to view details about a distribution configuration	Read	distributionConfiguration* (p. 739)		
GetImage	Grants permission to view details about an image	Read	image* (p. 739)		
				aws:ResourceTag/ \${TagKey} (p. 740)	
GetImagePipeline	Grants permission to view details about an image pipeline	Read	imagePipeline* (p. 740)		
GetImagePolicy	Grants permission to view the resource policy associated with an image	Read	image* (p. 739)		
GetImageRecipe	Grants permission to view details about an image recipe	Read	imageRecipe* (p. 739)		
GetImageRecipePolicy	Grants permission to view the resource policy associated with an image recipe	Read	imageRecipe* (p. 739)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetInfrastructureDetails	Grants permission to view details about an infrastructure configuration	Read	infrastructureConfiguration* (p. 740)		
ImportComponent	Grants permission to import a new component	Write	component* (p. 739) kmsKey (p. 740) aws:RequestTag/\${TagKey} (p. 740) aws:TagKeys (p. 740)		iam:CreateServiceLinkedRole imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithPlaintext
ImportVmImage	Grants permission to import an image	Write	image* (p. 739) aws:RequestTag/\${TagKey} (p. 740) aws:TagKeys (p. 740)	ec2:DescribeImportImage iam:CreateServiceLinkedRole	
ListComponentBuildVersions	Grants permission to list the component build versions in your account	List	componentVersion* (p. 739)		
ListComponents	Grants permission to list the component versions owned by or shared with your account	List			
ListContainerRecipes	Grants permission to list the container recipes owned by or shared with your account	List			
ListDistributionConfigurations	Grants permission to list the distribution configurations in your account	List			
ListImageBuildVersions	Grants permission to list the image build versions in your account	List	imageVersion* (p. 739)		
ListImagePackages	Grants permission to returns a list of packages installed on the specified image	List	image* (p. 739)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListImagePipeline	Grants permission to returns a list of images created by the specified pipeline	List	imagePipeline* (p. 740)		
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			
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			
ListTagsForResource	Grants permission to list tag for an Image Builder resource	Read	component (p. 739)		
distributionConfiguration (p. 739)					
image (p. 739)					
imagePipeline (p. 740)					
imageRecipe (p. 739)					
infrastructureConfiguration (p. 740)					
aws:ResourceTag/ \${TagKey} (p. 740)					
PutComponentPolicy	Grants permission to set the resource policy associated with a component	Permissions management	component* (p. 739)		
PutContainerRecipePolicy	Grants permission to set the resource policy associated with a container recipe		containerRecipe* (p. 739)		
PutImagePolicy	Grants permission to set the resource policy associated with an image	Permissions management	image* (p. 739)		
PutImageRecipePolicy	Grants permission to set the resource policy associated with an image recipe		imageRecipe* (p. 739)		
StartImagePipeline	Grants permission to create a new image from a pipeline	Write	imagePipeline* (p. 740)		iam:CreateServiceLinkedRole imagebuilder:GetImagePipeline
TagResource	Grants permission to tag an Image Builder resource	Tagging	component (p. 739)		
			containerRecipe (p. 739)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			distributionConfiguration (p. 739) image (p. 739) imagePipeline (p. 740) imageRecipe (p. 739) infrastructureConfiguration (p. 740)		
	Grants permission to untag an Image Builder resource	Tagging	aws:TagKeys (p. 740) aws:RequestTag/\${TagKey} (p. 740) aws:ResourceTag/\${TagKey} (p. 740)		
			component (p. 739)		
			containerRecipe (p. 739)		
			distributionConfiguration (p. 739)		
			image (p. 739)		
			imagePipeline (p. 740)		
			imageRecipe (p. 739)		
			infrastructureConfiguration (p. 740)		
			aws:ResourceTag/\${TagKey} (p. 740)		
			aws:TagKeys (p. 740)		
	UpdateDistribution an existing distribution configuration	Write	distributionConfiguration* (p. 739)		
	UpdateImagePipeline an existing image pipeline	Write	imagePipeline* (p. 740)		
	UpdateInfrastructure an existing infrastructure configuration	Write	infrastructureConfiguration (p. 740)	iam:PassRole sns:Publish	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/\${TagKey} (p. 740) imagebuilder:CreatedResourceTagKeys imagebuilder:CreatedResourceTag/<key> (p. 740) imagebuilder:Ec2MetadataHttpTokens imagebuilder:StatusTopicArn (p. 740)	

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 \(p. 732\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
component	<code>arn:\${Partition}:imagebuilder:\${Region}: \${Account}:component/\${ComponentName}/ \${ComponentVersion}/\${ComponentBuildVersion}</code>	aws:ResourceTag/\${TagKey} (p. 740)
componentVersion	<code>arn:\${Partition}:imagebuilder:\${Region}: \${Account}:component/\${ComponentName}/ \${ComponentVersion}</code>	aws:ResourceTag/\${TagKey} (p. 740)
distributionConfig	<code>arn:\${Partition}:imagebuilder:\${Region}: \${Account}:distribution-configuration/ \${DistributionConfigurationName}</code>	aws:ResourceTag/\${TagKey} (p. 740)
image	<code>arn:\${Partition}:imagebuilder: \${Region}: \${Account}:image/\${ImageName}/ \${ImageVersion}/\${ImageBuildVersion}</code>	aws:ResourceTag/\${TagKey} (p. 740)
imageVersion	<code>arn:\${Partition}:imagebuilder: \${Region}: \${Account}:image/\${ImageName}/ \${ImageVersion}</code>	aws:ResourceTag/\${TagKey} (p. 740)
imageRecipe	<code>arn:\${Partition}:imagebuilder:\${Region}: \${Account}:image-recipe/\${ImageRecipeName}/ \${ImageRecipeVersion}</code>	aws:ResourceTag/\${TagKey} (p. 740)
containerRecipe	<code>arn:\${Partition}:imagebuilder: \${Region}: \${Account}:container- recipe/\${ContainerRecipeName}/ \${ContainerRecipeVersion}</code>	aws:ResourceTag/\${TagKey} (p. 740)

Resource types	ARN	Condition keys
imagePipeline	arn:\${Partition}:imagebuilder:\${Region}:\${Account}:image-pipeline/\${ImagePipelineName}	aws:ResourceTag/\${TagKey} (p. 740)
infrastructureConfiguration	arn:\${Partition}:imagebuilder:\${Region}:\${Account}:infrastructure-configuration/\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 740)
kmsKey	arn:\${Partition}:kms:\${Region}:\${Account}:key/\${KeyId}	

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 [Available global condition 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:CreatedResourceTags<key>	Filters access by the tag key-value pairs attached to the resource tags created by Image Builder	String
imagebuilder:CreatedResourceTagKeys	Filters access by the presence of tag keys in the request	ArrayOfString
imagebuilder:Ec2MetadataTokenRequirements	Filters access by the EC2 Instance Metadata HTTP Token Requirements specified in the request	String
imagebuilder:StatusTerminal	Filters access by the SNS Topic Arn in the request to which terminal state notifications will be published	String

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 \(p. 741\)](#)
- [Resource types defined by Amazon EC2 Instance Connect \(p. 741\)](#)
- [Condition keys for Amazon EC2 Instance Connect \(p. 742\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendSSHPublicKey	Grants access to push an SSH public key to the specified EC2 instance to be used for standard SSH	Write	instance* (p. 741)		
			ec2:osuser (p. 742)		
SendSerialConsolePublicKey	Grants access to push an SSH public key to the specified EC2 instance to be used for serial console SSH	Write	instance* (p. 741)		

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 \(p. 741\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 742)

Resource types	ARN	Condition keys
		ec2:ResourceTag/\${TagKey} (p. 742)

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 [Available global condition keys](#).

Condition keys	Description	Type
aws:ResourceTag/\${TagKey}	Filters access based on the tags associated with the resource	String
ec2:ResourceTag/\${TagKey}	Filters access based on the 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 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 \(p. 742\)](#)
- [Resource types defined by AWS Elastic Beanstalk \(p. 748\)](#)
- [Condition keys for AWS Elastic Beanstalk \(p. 749\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 an in-progress environment configuration update or application version deployment	Write	environment*	elastictalk:InApplication (p. 749)	
AddTags	Grants permission to add tags to an Elastic Beanstalk resource and to update tag values	Tagging	application	(p. 748)	
			applicationversion	(p. 748)	
			configurationtemplate	(p. 748)	
			environment	(p. 749)	
			platform	(p. 749)	
			aws:RequestTag/ \${TagKey}	(p. 749)	
			aws:TagKeys	(p. 749)	
ApplyEnvironmentManagedAction	Grants permission to apply a scheduled managed action immediately	Write	environment*	elastictalk:InApplication (p. 749)	
AssociateEnvironmentWithOperationsRole	Grants permission to associate an operations role with an environment	Write	environment*	(p. 749)	
CheckDNSAvailability	Grants permission to check DNSNAME availability	Read			
ComposeEnvironmentUpdate	Grants permission to create or update a group of environments, each running a separate component of a single application	Write	application*	(p. 748)	
			applicationversion	elastictalk:InApplication (p. 749)	
CreateApplication	Grants permission to create a new application	Write	application*	(p. 748)	
			aws:RequestTag/ \${TagKey}	(p. 749)	
			aws:TagKeys	(p. 749)	
CreateApplicationVersion		Write	application*	(p. 748)	

Service Authorization Reference
Service Authorization Reference
AWS Elastic Beanstalk

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to create an application version for an application		application*	elasticbeanstalk:InApplication (p. 749)	
	Grants permission to create a configuration template	Write	configuration*	elasticbeanstalk:FromApplication (p. 749)	
	Grants permission to launch an environment for an application	Write	environment*	elasticbeanstalk:InApplication (p. 749)	
	Grants permission to create a new version of a custom platform	Write	platform* (p. 749)		
	Grants permission to create the Amazon S3 storage location for the account	Write			
	Grants permission to delete an application along with all associated versions and configurations	Write	application* (p. 748)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteApplicationVersion	Grants permission to delete an application version from an application	Write	applicationversion*	elasticbeanstalk:InApplication (p. 749)	
DeleteConfigurationTemplate	Grants permission to delete a configuration template	Write	configurationtemplate*	elasticbeanstalk:InApplication (p. 749)	
DeleteEnvironmentDraftConfiguration	Grants permission to delete the draft configuration associated with the running environment	Write	environment*	elasticbeanstalk:InApplication (p. 749)	
DeletePlatformVersion	Grants permission to delete a version of a custom platform	Write	platform* (p. 749)		
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 (p. 749)	
DescribeApplications	Grants permission to retrieve the descriptions of existing applications	List	application (p. 748)		
DescribeConfigurationOptions	Grants permission to retrieve descriptions of environment configuration options	Read	configurationoption*	elasticbeanstalk:InApplication (p. 749)	
DescribeConfigurationSettings	Grants permission to retrieve a description of the settings for a configuration set	Read	configurationsetting*	elasticbeanstalk:InApplication (p. 749)	
DescribeEnvironmentInformation	Grants permission to retrieve information about the overall health of an environment	Read	environment (p. 749)		
DescribeEnvironmentManagedActions	Grants permission to retrieve a list of environment's completed and failed managed actions	Read	environment*	elasticbeanstalk:InApplication (p. 749)	
DescribeEnvironmentManagedActionsHistory	Grants permission to retrieve a list of environment's upcoming and in-progress managed actions	Read	environment*	elasticbeanstalk:InApplication (p. 749)	
DescribeEnvironmentResources	Grants permission to retrieve a list of environment's AWS resources for an environment	Read	environment*	elasticbeanstalk:InApplication (p. 749)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeEnvironments	Grants permission to retrieve descriptions for existing environments	List	environment (p. 749)	elasticbeanstalk:InApplication (p. 749)	
DescribeEvents	Grants permission to retrieve a list of event descriptions matching a set of criteria	Read	application (p. 748)		
			applicationversion (p. 748)	elasticbeanstalk:InApplication (p. 749)	
			configurationtemplate (p. 748)	elasticbeanstalk:InApplication (p. 749)	
			environment (p. 749)	elasticbeanstalk:InApplication (p. 749)	
DescribeInstances	Grants permission to retrieve more detailed information about the health of environment instances	Read	environment (p. 749)		
DescribePlatformVersion	Grants permission to retrieve a description of a platform version	Read	platform (p. 749)		
DisassociateEnvironment	Grants permission to disassociate an application role with an environment	Write	environment* (p. 749)		
ListAvailableSolutionStacks	Grants permission to retrieve a list of the available solution stack names	List	solutionstack (p. 749)		
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 (p. 749)		
ListTagsForResource	Grants permission to retrieve a list of tags of an Elastic Beanstalk resource	Read	application (p. 748)		
			applicationversion (p. 748)		
			configurationtemplate (p. 748)		
			environment (p. 749)		
			platform (p. 749)		
PutInstanceStatistics	Grants permission to submit instance statistics for enhanced health	Write	application* (p. 748)		
			environment* (p. 749)		
RebuildEnvironment	Grants permission to delete and recreate all of the AWS resources for an environment and to force a restart	Write	environment* (p. 749)	elasticbeanstalk:InApplication (p. 749)	
RemoveTags	Grants permission to remove tags from an Elastic Beanstalk resource	Tagging	application (p. 748)		
			applicationversion (p. 748)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			configurationtemplate (p. 748)		
			environment (p. 749)		
			platform (p. 749)		
			aws:TagKeys (p. 749)		
RequestEnvironmentInfo	Grants permission to initiate a <code>RequestEnvironmentInfo</code> request to compile information of the deployed environment	Read	environment* (p. 749)	elasticbeanstalk:InApplication (p. 749)	
RestartAppServer	Grants permission to request an environment to restart the application container server running on each Amazon EC2 instance	Write	environment* (p. 749)	elasticbeanstalk:InApplication (p. 749)	
RetrieveEnvironmentInfo	Grants permission to retrieve the compiled information from a <code>RequestEnvironmentInfo</code> request	Read	environment* (p. 749)	elasticbeanstalk:InApplication (p. 749)	
SwapEnvironmentCNAMES	Grants permission to swap the CNAMEs of two environments	Write	environment* (p. 749)	elasticbeanstalk:InApplication (p. 749)	
TerminateEnvironment	Grants permission to terminate an environment		environment* (p. 749)	elasticbeanstalk:FromEnvironment (p. 749)	
UpdateApplication	Grants permission to update an application with specified properties	Write	application* (p. 748)		
UpdateApplicationLifecycle	Grants permission to update the application version lifecycle policy associated with the application	Write	application* (p. 748)		
UpdateApplicationVersion	Grants permission to update an application version with specified properties	Write	applicationversion* (p. 748)	elasticbeanstalk:InApplication (p. 749)	
UpdateConfigurationTemplate	Grants permission to update a configuration template with specified properties or configuration option values	Write	configurationtemplate* (p. 748)	elasticbeanstalk:Application (p. 749)	
			elasticbeanstalk:FromApplication (p. 749)	elasticbeanstalk:FromApplicationVersion (p. 749)	
			elasticbeanstalk:FromConfigurationTemplate (p. 749)	elasticbeanstalk:FromEnvironment (p. 749)	
			elasticbeanstalk:FromSolutionStack (p. 749)	elasticbeanstalk:FromPlatform (p. 749)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateEnvironment	Grants permission to update an environment	Write	environment (p. 749)	elasticbeanstalk:InApplication (p. 749)	
UpdateTagsForResource	Grants permission to add tags to an Elastic Beanstalk resource, remove tags, and to update tag values	Tagging	application (p. 748) applicationversion (p. 748) configurationtemplate (p. 748) environment (p. 749) platform (p. 749) aws:RequestTag/ {\$TagKey} (p. 749) aws:TagKeys (p. 749)		
ValidateConfigurationSettings	Grants permission to check the validity of a set of configuration settings for a configuration template or an environment	Read	configurationtemplate (p. 748) environment (p. 749)	elasticbeanstalk:InApplication (p. 749)	

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 \(p. 742\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
application	<code>arn:\${Partition}:elasticbeanstalk:\${Region}: \${Account}:application/\${ApplicationName}</code>	aws:ResourceTag/ {\$TagKey} (p. 749)
applicationversion	<code>arn:\${Partition}:elasticbeanstalk: \${Region}: \${Account}:applicationversion/ \${ApplicationName}/\${VersionLabel}</code>	aws:ResourceTag/ {\$TagKey} (p. 749) elasticbeanstalk:InApplication (p. 749)
configurationtemplate	<code>arn:\${Partition}:elasticbeanstalk: \${Region}: \${Account}:configurationtemplate/ \${ApplicationName}/\${TemplateName}</code>	aws:ResourceTag/ {\$TagKey} (p. 749) elasticbeanstalk:InApplication (p. 749)

Resource types	ARN	Condition keys
environment	arn:\${Partition}:elasticbeanstalk:\${Region}: \${Account}:environment/\${ApplicationName}/ \${EnvironmentName}	aws:ResourceTag/\${TagKey} (p. 749) elasticbeanstalk:InApplication (p. 749)
solutionstack	arn:\${Partition}:elasticbeanstalk: \${Region}::solutionstack/ \${SolutionStackName}	
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 [Available global condition 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:FrontendConstraint	Filters access by an application as a dependency or a constraint on an input parameter	ARN
elasticbeanstalk:FrontendVersion	Filters access by an application version as a dependency or a constraint on an input parameter	ARN
elasticbeanstalk:FrontendTemplateName	Filters access by a configuration template as a dependency or a constraint on an input parameter	ARN
elasticbeanstalk:FrontendEnvironment	Filters access by an environment as a dependency or a constraint on an input parameter	ARN
elasticbeanstalk:FrontendPlatform	Filters access by a platform as a dependency or a constraint on an input parameter	ARN
elasticbeanstalk:FrontendSolutionStack	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 \(p. 750\)](#)
- [Resource types defined by Amazon Elastic Block Store \(p. 751\)](#)
- [Condition keys for Amazon Elastic Block Store \(p. 752\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 751)		
				aws:ResourceTag/\${TagKey} (p. 752)	
GetSnapshotBlock	Grants permission to return the data of a block in an Amazon Elastic Block Store (EBS) snapshot	Read	snapshot* (p. 751)		
				aws:ResourceTag/\${TagKey} (p. 752)	
ListChangedBlock	Grants permission to list the blocks that are different between two Amazon Elastic	Read	snapshot* (p. 751)		
				aws:ResourceTag/\${TagKey} (p. 752)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Block Store (EBS) snapshots of the same volume/snapshot lineage				
ListSnapshotBlocks	Grants permission to list the blocks in an Amazon Elastic Block Store (EBS) snapshot	Read	snapshot* (p. 751)		
				aws:ResourceTag/\${TagKey} (p. 752)	
PutSnapshotBlock	Grants permission to write a block of data to a snapshot created by the StartSnapshot operation	Write	snapshot* (p. 751)		
				aws:ResourceTag/\${TagKey} (p. 752)	
StartSnapshot	Grants permission to create a new EBS snapshot	Write	snapshot (p. 751)		
				aws:RequestTag/\${TagKey} (p. 752)	
				aws:ResourceTag/\${TagKey} (p. 752)	
				aws:TagKeys (p. 752)	
				ebs:Description (p. 752)	
				ebs:ParentSnapshot (p. 752)	
				ebs:VolumeSize (p. 752)	

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 \(p. 750\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 752) aws:ResourceTag/\${TagKey} (p. 752) aws:TagKeys (p. 752) ebs:Description (p. 752) ebs:ParentSnapshot (p. 752) ebs:VolumeSize (p. 752)

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 [Available global condition 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 based on tag key-value pairs assigned to the AWS resource	String
aws:TagKeys	Filters access by a list of tag keys that are allowed in the request	String
ebs:Description	Filters access by the description of the snapshot being created	String
ebs:ParentSnapshot	Filters access by the ID of the parent snapshot	String
ebs:VolumeSize	Filters access by the size of the volume for the snapshot being created, in GiB	Numeric

Actions, resources, and condition keys for Amazon Elastic Container Registry

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

References:

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

Topics

- [Actions defined by Amazon Elastic Container Registry \(p. 752\)](#)
- [Resource types defined by Amazon Elastic Container Registry \(p. 756\)](#)
- [Condition keys for Amazon Elastic Container Registry \(p. 756\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 756)		
BatchDeleteImage	Grants permission to delete a list of specified images within a specified repository	Write	repository* (p. 756)		
BatchGetImage	Grants permission to get detailed information for specified images within a specified repository	Read	repository* (p. 756)		
BatchGetRepositoryScanningConfig	Grants permission to retrieve repository scanning configuration for a list of repositories	Read	repository* (p. 756)		
BatchImportUpstreamImage	Grants permission to retrieve the image from the upstream registry and import it to your private registry	Write			
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* (p. 756)		
CreatePullThroughCacheRule	Grants permission to create new pull-through cache rule	Write			
CreateRepository	Grants permission to create an image repository	Write		aws:RequestTag/\${TagKey} (p. 756) aws:TagKeys (p. 757)	
DeleteLifecyclePolicy	Grants permission to delete the specified lifecycle policy	Write	repository* (p. 756)		
DeletePullThroughCacheRule	Grants permission to delete the pull-through cache rule	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteRegistryPolicy	Grants permission to delete the registry policy	Permissions management			
DeleteRepository	Grants permission to delete an existing image repository	Write	repository* (p. 756)		
DeleteRepositoryPolicy	Grants permission to delete the repository policy from a specified repository	Permissions management	repository* (p. 756)		
DescribeImageReplicationStatus	Grants permission to retrieve replication status about an image in a registry, including failure reason if replication fails	Read	repository* (p. 756)		
DescribeImageScanFindings	Grants permission to describe the scan findings for the specified image	Read	repository* (p. 756)		
DescribeImages	Grants permission to get metadata about the images in a repository, including image size, image tags, and creation date	List	repository* (p. 756)		
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 (p. 756)		
GetAuthorizationToken	Grants permission to retrieve a token that is valid for a specified registry for 12 hours	Read			
GetDownloadUrl	Grants permission to retrieve the download URL corresponding to an image layer	Read	repository* (p. 756)		
GetLifecyclePolicy	Grants permission to retrieve the specified lifecycle policy	Read	repository* (p. 756)		
GetLifecyclePolicyPreview	Grants permission to retrieve the results of the specified lifecycle policy preview request	Read	repository* (p. 756)		
GetRegistryPolicy	Grants permission to retrieve the registry policy	Read			
GetRegistryScanningConfiguration	Grants permission to retrieve registry scanning configuration	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRepositoryPolicy	Grants permission to retrieve the repository policy for a specified repository	Read	repository* (p. 756)		
InitiateLayerUpload	Grants permission to notify Amazon ECR that you intend to upload an image layer	Write	repository* (p. 756)		
ListImages	Grants permission to list all the image IDs for a given repository	List	repository* (p. 756)		
ListTagsForResource	Grants permission to list the tags for an Amazon ECR resource	Read	repository* (p. 756)		
				aws:RequestTag/\${TagKey} (p. 756)	
PutImage	Grants permission to create or update the image manifest associated with an image	Write	repository* (p. 756)		
PutImageScanningConfiguration	Grants permission to update the image scanning configuration for a repository	Write	repository* (p. 756)		
PutImageTagMutability	Grants permission to update the image tag mutability settings for a repository	Write	repository* (p. 756)		
PutLifecyclePolicy	Grants permission to create or update a lifecycle policy	Write	repository* (p. 756)		
PutRegistryPolicy	Grants permission to update the registry policy	Permissions management			
PutRegistryScanningConfiguration	Grants permission to update the registry scanning configuration	Write			
PutReplicationConfiguration	Grants permission to update the replication configuration for the registry	Write			
ReplicateImage	Grants permission to replicate images to the destination registry	Write	repository* (p. 756)		
SetRepositoryPolicy	Grants permission to apply a repository policy on a specified repository to control access permissions	Permissions management	repository* (p. 756)		
StartImageScan	Grants permission to start an image scan	Write	repository* (p. 756)		

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* (p. 756)		
TagResource	Grants permission to tag an Amazon ECR resource	Tagging	repository* (p. 756)		
				aws:RequestTag/ {\$TagKey} (p. 756) aws:TagKeys (p. 757)	
UntagResource	Grants permission to untag an Amazon ECR resource	Tagging	repository* (p. 756)		
				aws:RequestTag/ {\$TagKey} (p. 756) aws:TagKeys (p. 757)	
UploadLayerPart	Grants permission to upload an image layer part to Amazon ECR	Write	repository* (p. 756)		

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 \(p. 752\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 757) ecr:ResourceTag/ {\$TagKey} (p. 757)

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 [Available global condition keys](#).

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

Condition keys	Description	Type
aws:ResourceTag/\${TagKey}	Filters access by tag-value associated with the resource	String
aws:TagKeys	Filters access by the presence of mandatory tags in the request	ArrayOfString
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 \(p. 757\)](#)
- [Resource types defined by Amazon Elastic Container Registry Public \(p. 759\)](#)
- [Condition keys for Amazon Elastic Container Registry Public \(p. 760\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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	Read	repository* (p. 760)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	layers in a specified registry and repository				
BatchDeleteImage	Grants permission to delete a list of specified images within a specified repository	Write	repository* (p. 760)		
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* (p. 760)		
CreateRepository	Grants permission to create an image repository	Write	repository* (p. 760)		
				aws:RequestTag/ \${TagKey} (p. 760)	
				aws:TagKeys (p. 760)	
DeleteRepository	Grants permission to delete an existing image repository	Write	repository* (p. 760)		
DeleteRepositoryPolicy	Grants permission to delete the repository policy from a specified repository	Write	repository* (p. 760)		
DescribeImageTags	Grants permission to describe all the image tags for a given repository	List	repository* (p. 760)		
DescribeImages	Grants permission to get metadata about the images in a repository, including image size, image tags, and creation date	Read	repository* (p. 760)		
DescribeRegistries	Grants permission to retrieve the catalog data associated with a registry	List	registry* (p. 760)		
DescribeRepositories	Grants permission to describe image repositories in a registry	List	repository (p. 760)		
GetAuthorizationToken	Grants permission to retrieve a token that is valid for a specified registry for 12 hours	Read			
GetRegistryCatalog	Grants permission to retrieve the catalog data associated with a registry	Read	registry* (p. 760)		
GetRepositoryCatalog	Grants permission to retrieve the catalog data associated with a repository	Read	repository* (p. 760)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRepositoryPolicy	Grants permission to retrieve the repository policy for a specified repository	Read	repository* (p. 760)		
InitiateLayerUpload	Grants permission to notify Amazon ECR that you intend to upload an image layer	Write	repository* (p. 760)		
ListTagsForResource	Grants permission to list the tags for an Amazon ECR resource	Read	repository* (p. 760)		
PutImage	Grants permission to create or update the image manifest associated with an image	Write	repository* (p. 760)		
PutRegistryCatalogData	Grants permission to create and update the catalog data associated with a registry	Write	registry* (p. 760)		
PutRepositoryCatalogData	Grants permission to update the catalog data associated with a repository	Write	repository* (p. 760)		
SetRepositoryPolicy	Grants permission to apply a repository policy on a specified repository to control access permissions	Permissions management	repository* (p. 760)		
TagResource	Grants permission to tag an Amazon ECR resource	Tagging	repository* (p. 760)		
					aws:RequestTag/ \${TagKey} (p. 760)
UntagResource	Grants permission to untag an Amazon ECR resource	Tagging	repository* (p. 760)		
					aws:RequestTag/ \${TagKey} (p. 760)
UploadLayerPart	Grants permission to upload an image layer part to Amazon ECR Public	Write	repository* (p. 760)		

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 \(p. 757\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 760) ecr-public:ResourceTag/\${TagKey} (p. 760)
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 [Available global condition 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 \(p. 761\)](#)
- [Resource types defined by Amazon Elastic Container Service \(p. 768\)](#)
- [Condition keys for Amazon Elastic Container Service \(p. 769\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCapacityProvider	Grants permission to create a new capacity provider. Capacity providers are associated with an Amazon ECS cluster and are used in capacity provider strategies to facilitate cluster auto scaling	Write		aws:RequestTag/\${TagKey} (p. 769) aws:TagKeys (p. 769)	
CreateCluster	Grants permission to create a new Amazon ECS cluster	Write		ecs:capacity-provider (p. 769) aws:RequestTag/\${TagKey} (p. 769) aws:TagKeys (p. 769)	
CreateService	Grants permission to run and maintain a desired number of tasks from a specified task definition via service creation	Write	service* (p. 768)	ecs:cluster (p. 769) ecs:capacity-provider (p. 769) ecs:task-definition (p. 769) ecs:enable-execute-command (p. 769) aws:RequestTag/\${TagKey} (p. 769) aws:TagKeys (p. 769)	
CreateTaskSet	Grants permission to create a new Amazon ECS task set	Write		ecs:cluster (p. 769)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ecs:capacity-provider (p. 769)	
	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:service (p. 769)	
DeleteAttributes	Grants permission to delete one or more custom attributes from an Amazon ECS resource	Write	container-instance* (p. 768)		
				ecs:cluster (p. 769)	
DeleteCapacityProvider	Grants permission to delete the specified capacity provider	Write	capacity-provider* (p. 768)		
DeleteCluster	Grants permission to delete the specified cluster	Write	cluster* (p. 768)		
DeleteService	Grants permission to delete a specified service within a cluster	Write	service* (p. 768)		
				ecs:cluster (p. 769)	
DeleteTaskSet	Grants permission to delete the specified task set	Write	task-set* (p. 768)		
				ecs:cluster (p. 769)	
				ecs:service (p. 769)	
DeregisterContainerInstances	Grants permission to deregister an Amazon ECS container instance from the specified cluster	Write	cluster* (p. 768)		
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* (p. 768)		
DescribeClusters	Grants permission to describes one or more of your clusters	Read	cluster* (p. 768)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeContainerInstances	Grants permission to describe Amazon ECS container instances	Read	container-instance* (p. 768)		
				ecs:cluster (p. 769)	
DescribeServices	Grants permission to describe the specified services running in your cluster	Read	service* (p. 768)		
				ecs:cluster (p. 769)	
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* (p. 768)		
				ecs:cluster (p. 769)	ecs:service (p. 769)
DescribeTasks	Grants permission to describe a specified task or tasks	Read	task* (p. 768)		
				ecs:cluster (p. 769)	
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 (p. 768)		
			task (p. 768)		
				ecs:cluster (p. 769)	
				ecs:container-name (p. 769)	
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* (p. 768)		
ListClusters	Grants permission to get a list of existing clusters	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListContainerInstances	Grants permission to get a list of container instances in a specified cluster	List	cluster* (p. 768)		
ListServices	Grants permission to get a list of services that are running in a specified cluster	List		ecs:cluster (p. 769)	
ListTagsForResource	Grants permission to get a list of tags for the specified resource	Read	cluster (p. 768)		
			container-instance (p. 768)		
			task (p. 768)		
			task-definition (p. 768)		
ListTaskDefinitionList	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			
ListTaskDefinitionList	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* (p. 768)		
				ecs:cluster (p. 769)	
Poll [permission only]	Grants permission to an agent to connect with the Amazon ECS service to report status and get commands	Write	container-instance* (p. 768)		
				ecs:cluster (p. 769)	
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			

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 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			
PutAttributes	Grants permission to create or update an attribute on an Amazon ECS resource	Write	container-instance* (p. 768)		
				ecs:cluster (p. 769)	
PutClusterCapacityProvider	Grants permission to modify the capacity providers and the default capacity provider strategy for a cluster	Write	capacity-provider* (p. 768)		
				ecs:capacity-provider (p. 769)	
RegisterContainerInstance	Grants permission to register an EC2 instance into the specified cluster	Write	cluster* (p. 768)		
				aws:RequestTag/\${TagKey} (p. 769)	
				aws:TagKeys (p. 769)	
RegisterTaskDefinition	Grants permission to register a new task definition from the supplied family and containerDefinitions	Write		aws:RequestTag/\${TagKey} (p. 769)	
RunTask	Grants permission to start a task using random placement and the default Amazon ECS scheduler	Write	task-definition* (p. 768)		
				ecs:cluster (p. 769)	
				ecs:capacity-provider (p. 769)	
				ecs:enable-execute-command (p. 769)	
				aws:RequestTag/\${TagKey} (p. 769)	
				aws:TagKeys (p. 769)	

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* (p. 768)		
			ecs:cluster (p. 769)		
			ecs:container-instances (p. 769)		
			ecs:enable-execute-command (p. 769)		
			aws:RequestTag/\${TagKey} (p. 769)		
			aws:TagKeys (p. 769)		
StartTelemetrySession	Grants permission to start a telemetry session	Write	container-instance* (p. 768)		
			ecs:cluster (p. 769)		
StopTask	Grants permission to stop a running task	Write	task* (p. 768)		
			ecs:cluster (p. 769)		
SubmitAttachmentAcknowledgment	Grants permission to send acknowledgement that attachments changed states	Write	cluster* (p. 768)		
SubmitContainerStateAcknowledgment	Grants permission to send acknowledgement that a container changed states	Write	cluster* (p. 768)		
SubmitTaskStateAcknowledgment	Grants permission to send an acknowledgement that a task changed states	Write	cluster* (p. 768)		
TagResource	Grants permission to tag the specified resource	Tagging	cluster (p. 768)		
	container-instance (p. 768)				
	service (p. 768)				
	task (p. 768)				
	task-definition (p. 768)				
			aws:TagKeys (p. 769)		
			aws:RequestTag/\${TagKey} (p. 769)		
UntagResource	Grants permission to untag the specified resource	Tagging	cluster (p. 768)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			container-instance (p. 768) service (p. 768) task (p. 768) task-definition (p. 768)		
				aws:TagKeys (p. 769) aws:RequestTag/\${TagKey} (p. 769)	
UpdateCapacityProvider	Grants permission to update the specified capacity provider	Write	capacity-provider* (p. 768)		
UpdateCluster	Grants permission to modify the configuration or settings to use for a cluster	Write	cluster* (p. 768)		
UpdateClusterSetting	Grants permission to modify the settings to use for a cluster	Write	cluster* (p. 768)		
UpdateContainerAgent	Grants permission to update the Amazon ECS container agent on a specified container instance	Write	container-instance* (p. 768) ecs:cluster (p. 769)		
UpdateContainerInstanceStatus	Grants permission to the user to modify the status of an Amazon ECS container instance	Write	container-instance* (p. 768) ecs:cluster (p. 769)		
UpdateService	Grants permission to modify the parameters of a service	Write	service* (p. 768) ecs:cluster (p. 769) ecs:capacity-provider (p. 769) ecs:enable-execute-command (p. 769) ecs:task-definition (p. 769)		
UpdateServicePrimaryTask	Grants permission to modify the primary task set used in a service	Write	service* (p. 768) ecs:cluster (p. 769)		
UpdateTaskSet	Grants permission to update the specified task set	Write	task-set* (p. 768)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ecs:cluster (p. 769) ecs:service (p. 769)	

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 \(p. 761\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
<code>cluster</code>	<code>arn:\${Partition}:ecs:\${Region}: \${Account}:cluster/\${ClusterName}</code>	<code>aws:ResourceTag/\${TagKey}</code> (p. 769) <code>ecs:ResourceTag/\${TagKey}</code> (p. 769)
<code>container-instance</code>	<code>arn:\${Partition}:ecs:\${Region}: \${Account}:container-instance/ \${ClusterName}/\${ContainerInstanceId}</code>	<code>aws:ResourceTag/\${TagKey}</code> (p. 769) <code>ecs:ResourceTag/\${TagKey}</code> (p. 769)
<code>service</code>	<code>arn:\${Partition}:ecs:\${Region}: \${Account}:service/\${ClusterName}/ \${ServiceName}</code>	<code>aws:ResourceTag/\${TagKey}</code> (p. 769) <code>ecs:ResourceTag/\${TagKey}</code> (p. 769)
<code>task</code>	<code>arn:\${Partition}:ecs:\${Region}: \${Account}:task/\${ClusterName}/\${TaskId}</code>	<code>aws:ResourceTag/\${TagKey}</code> (p. 769) <code>ecs:ResourceTag/\${TagKey}</code> (p. 769)
<code>task-definition</code>	<code>arn:\${Partition}:ecs:\${Region}: \${Account}:task-definition/ \${TaskDefinitionFamilyName}: \${TaskDefinitionRevisionNumber}</code>	<code>aws:ResourceTag/\${TagKey}</code> (p. 769) <code>ecs:ResourceTag/\${TagKey}</code> (p. 769)
<code>capacity-provider</code>	<code>arn:\${Partition}:ecs:\${Region}: \${Account}:capacity-provider/ \${CapacityProviderName}</code>	<code>aws:ResourceTag/\${TagKey}</code> (p. 769) <code>ecs:ResourceTag/\${TagKey}</code> (p. 769)
<code>task-set</code>	<code>arn:\${Partition}:ecs:\${Region}: \${Account}:task-set/\${ClusterName}/ \${ServiceName}/\${TaskSetId}</code>	<code>aws:ResourceTag/\${TagKey}</code> (p. 769)

Resource types	ARN	Condition keys
		ecs:ResourceTag/\${TagKey} (p. 769)

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 [Available global condition 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	String
ecs:ResourceTag/\${TagKey}	Filters access by the tag key-value pairs attached to the resource	String
ecs:capacity-provider	Filters access by the ARN of an Amazon ECS capacity provider	ARN
ecs:cluster	Filters access by the ARN of an Amazon ECS cluster	ARN
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-execute-command	Filters access by the execute-command capability of your Amazon ECS task or Amazon ECS service	String
ecs:service	Filters access by the ARN of an Amazon ECS service	ARN
ecs:task	Filters access by the ARN of an Amazon ECS task	ARN
ecs:task-definition	Filters access by the ARN of an Amazon ECS task definition	ARN

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 \(p. 770\)](#)
- [Resource types defined by AWS Elastic Disaster Recovery \(p. 777\)](#)
- [Condition keys for AWS Elastic Disaster Recovery \(p. 778\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateFallbackClientForDrs [permission only]	Grants permission to get <code>AssociateFallbackClientForDrs</code> recovery instance	Write	RecoveryInstanceResource* (p. 778)		
BatchCreateVolumeSnapshotGroup [permission only]	Grants permission to batch <code>CreateVolumeSnapshotGroup</code>	Write	RecoveryInstanceResource* (p. 778)		
			SourceServerResource* (p. 778)		
BatchDeleteSnapshotRequest [permission only]	Grants permission to batch <code>DeleteSnapshotRequest</code>	Write			
CreateConvertedSnapshot [permission only]	Grants permission to create <code>ConvertedSnapshot</code>	Write	SourceServerResource* (p. 778)		
				aws:RequestTag/\${TagKey} (p. 778)	
				aws:TagKeys (p. 778)	
CreateExtendedSnapshot [permission only]	Grants permission to extend a <code>sourceServer</code>	Write		aws:RequestTag/\${TagKey} (p. 778)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					aws:TagKeys (p. 778)
CreateRecoveryInstance [permission only]	Grants permission to create <code>recoveryInstance</code>	Write	SourceServerResource* (p. 778)		aws:RequestTag/\${TagKey} (p. 778) aws:TagKeys (p. 778)
CreateReplicationConfiguration	Grants permission to create <code>replicationConfiguration</code> template	Write			aws:RequestTag/\${TagKey} (p. 778) aws:TagKeys (p. 778)
CreateSessionForRecovery	Grants permission to create a <code>Session</code>	Write			
CreateSourceServer [permission only]	Grants permission to create a <code>sourceServer</code>	Write			aws:RequestTag/\${TagKey} (p. 778) aws:TagKeys (p. 778)
DeleteJob	Grants permission to delete a job	Write	JobResource* (p. 777)		
DeleteRecoveryInstance	Grants permission to delete <code>recovery instance</code>	Write	RecoveryInstanceResource* (p. 778)		
DeleteReplicationConfiguration	Grants permission to delete <code>replicationConfiguration</code> template	Write	ReplicationConfigurationTemplateResource* (p. 778)		
DeleteSourceServer	Grants permission to delete <code>source server</code>	Write	SourceServerResource* (p. 778)		
DescribeJobLogItems	Grants permission to describe <code>job log items</code>	Read	JobResource* (p. 777)		
DescribeJobs	Grants permission to describe jobs	Read			
DescribeRecoveryInstances	Grants permission to describe <code>recovery instances</code>	Read			ec2:DescribeInstances
DescribeRecoverySnapshots	Grants permission to describe <code>recovery snapshots</code>	Read	SourceServerResource* (p. 778)		
DescribeReplicationConfigurations	Grants permission to describe <code>replication configurations</code> template	Read			
DescribeReplicationServerAssociations [permission only]	Grants permission to describe <code>replication server associations</code>	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeSnapshotRequests [permission only]	Grants permission to describe snapshot requests	Read			
DescribeSourceServers	Grants permission to describe source servers	Read			
DisconnectRecoveryInstance	Grants permission to disconnect recovery instance	Write	RecoveryInstanceResource* (p. 778)		
DisconnectSourceServer	Grants permission to disconnect source server	Write	SourceServerResource* (p. 778)		
GetAgentCommand [permission only]	Grants permission to get agent command	Read	RecoveryInstanceResource* (p. 778)		
GetAgentConfirmedInfo [permission only]	Grants permission to get agent confirmed info		SourceServerResource* (p. 778)		
GetAgentInstallationAssets [permission only]	Grants permission to get agent installation assets	Read	RecoveryInstanceResource* (p. 778)		
GetAgentReplicationInfo [permission only]	Grants permission to get agent replication info	Read	RecoveryInstanceResource* (p. 778)	SourceServerResource* (p. 778)	
GetAgentRuntimeConfiguration [permission only]	Grants permission to get agent runtime configuration		RecoveryInstanceResource* (p. 778)	SourceServerResource* (p. 778)	
GetAgentSnapshotCredits [permission only]	Grants permission to get agent snapshot credits	Read	RecoveryInstanceResource* (p. 778)	SourceServerResource* (p. 778)	
GetChannelCommands [permission only]	Grants permission to get channel commands		RecoveryInstanceResource* (p. 778)		
GetFallbackCommands [permission only]	Grants permission to get fallback commands	Read	RecoveryInstanceResource* (p. 778)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetFallbackLaunchRequested [permission only]	Grants permission to get <code>fallbackLaunchRequested</code>	Read	RecoveryInstanceResource* (p. 778)		
GetFallbackReplication [permission only]	Grants permission to get <code>fallbackReplication</code> configuration	Read	RecoveryInstanceResource* (p. 778)		
GetLaunchConfiguration [permission only]	Grants permission to get launch configuration	Read	SourceServerResource* (p. 778)		
GetReplicationConfiguration [permission only]	Grants permission to get replication configuration	Read	SourceServerResource* (p. 778)		
GetSuggestedFallbackClientDevices [permission only]	Grants permission to get suggested fallback client devices mapping	Read	RecoveryInstanceResource* (p. 778)		
InitializeService	Grants permission to initialize service	Write			iam:AddRoleToInstanceProfile iam:CreateInstanceProfile iam:CreateServiceLinkedRole iam:GetInstanceProfile
IssueAgentCertificate [agent certificate]	Grants permission to issue an agent certificate	Write	RecoveryInstanceResource* (p. 778) SourceServerResource* (p. 778)		
ListExtensibleSources	Grants permission to list extensible source servers	Read			
ListStagingAccounts	Grants permission to list staging accounts	Read			
ListTagsForResource	Grants permission to list tags for resource	Read			
NotifyAgentAuthentication [agent authentication]	Grants permission to notify agent authentication	Write	RecoveryInstanceResource* (p. 778) SourceServerResource* (p. 778)		
NotifyAgentConnection [agent connection]	Grants permission to notify agent connection	Write	RecoveryInstanceResource* (p. 778) SourceServerResource* (p. 778)		
NotifyAgentDisconnection [agent disconnection]	Grants permission to notify agent disconnection	Write	RecoveryInstanceResource* (p. 778) SourceServerResource* (p. 778)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
NotifyAgentReplicationProgress [permission only]	Grants permission to notify agent Replication Progress	Write	RecoveryInstanceResource* (p. 778)		
			SourceServerResource* (p. 778)		
NotifyConsistencyAttained [permission only]	Grants permission to notify consistency attained	Write	RecoveryInstanceResource* (p. 778)		
NotifyReplicationServerAuthentication [permission only]	Grants permission to notify Replication server authentication	Write	RecoveryInstanceResource* (p. 778)		
RetryDataReplication	Grants permission to retry data replication	Write	SourceServerResource* (p. 778)		
SendAgentLogsForLogs [permission only]	Grants permission to send agent logs	Write	RecoveryInstanceResource* (p. 778)		
			SourceServerResource* (p. 778)		
SendAgentMetricsForMetrics [permission only]	Grants permission to send agent metrics	Write	RecoveryInstanceResource* (p. 778)		
			SourceServerResource* (p. 778)		
SendChannelCommandForCommand [permission only]	Grants permission to send channel command result	Write			
SendClientLogsForLogs [permission only]	Grants permission to send client logs	Write			
SendClientMetricsForMetrics [permission only]	Grants permission to send client metrics	Write			
StartFallbackLaunchForLaunch	Grants permission to start fallback launch	Write	RecoveryInstanceResource* (p. 778)		
			aws:RequestTag/\${TagKey} (p. 778) aws:TagKeys (p. 778)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartRecovery	Grants permission to start recovery	Write	SourceServerResource* (p:drsc:CreateRecoveryInstance)		drs:ListTagsForResource ec2:AttachVolume ec2:AuthorizeSecurityGroupIngress ec2:AuthorizeSecurityGroupEgress ec2>CreateLaunchTemplate ec2>CreateLaunchTemplateVersion ec2>CreateSnapshot ec2>CreateTags ec2>CreateVolume ec2>DeleteLaunchTemplate ec2>DeleteSnapshot ec2>DeleteVolume ec2:DescribeAccountAttributes ec2:DescribeAvailabilityZones ec2:DescribeImages ec2:DescribeInstanceAttribute ec2:DescribeInstanceState ec2:DescribeInstanceTypeOfferings ec2:DescribeInstances ec2:DescribeLaunchTemplateVersions ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSnapshots ec2:DescribeSubnets ec2:DescribeVolumes ec2:DetachVolume ec2:ModifyInstanceAttribute ec2:ModifyLaunchTemplate

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:RevokeSecurityGroups ec2:RunInstances ec2:StartInstances ec2:StopInstances ec2:TerminateInstances iam:PassRole
	aws:RequestTag/ \${TagKey} (p. 778)				
StopFallback	Grants permission to stop failback	Write	RecoveryInstanceResource* (p. 778)		
TagResource	Grants permission to assign a resource tag	Tagging		aws:RequestTag/ \${TagKey} (p. 778) aws:TagKeys (p. 778) drs>CreateAction (p. 778)	
TerminateRecoveryInstances	Grants permission to terminate recovery instances	Write	RecoveryInstanceResource* (p. 778)		ec2:DeleteVolume ec2:DescribeInstances ec2:DescribeVolumes ec2:TerminateInstances
	aws:RequestTag/ \${TagKey} (p. 778) aws:TagKeys (p. 778)				
UntagResource	Grants permission to untag a resource	Tagging			aws:TagKeys (p. 778)
UpdateAgentBacklog [permission only]	Grants permission to update agent backlog	Write	RecoveryInstanceResource* (p. 778)		
	SourceServerResource* (p. 778)				
UpdateAgentConversionInfo [permission only]	Grants permission to update agent conversion info	Write	RecoveryInstanceResource* (p. 778)		
	SourceServerResource* (p. 778)				
UpdateAgentReplicationInfo [permission only]	Grants permission to update agent replication info	Write	RecoveryInstanceResource* (p. 778)		
	SourceServerResource* (p. 778)				

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAgentReplicaProperties [permission only]	Grants permission to update agent replication properties state	Write	RecoveryInstanceResource* (p. 778)		
			SourceServerResource* (p. 778)		
UpdateAgentSourceProperties [permission only]	Grants permission to update agent source properties	Write	RecoveryInstanceResource* (p. 778)		
			SourceServerResource* (p. 778)		
UpdateFallbackClientDeviceMapping [permission only]	Grants permission to update fallback client device mapping	Write	RecoveryInstanceResource* (p. 778)		
UpdateFallbackClientLastSeen [permission only]	Grants permission to update fallback client last seen	Write	RecoveryInstanceResource* (p. 778)		
UpdateFallbackReplicationConfiguration	Grants permission to update fallback replication configuration	Write	RecoveryInstanceResource* (p. 778)		
UpdateLaunchConfiguration	Grants permission to update launch configuration	Write	SourceServerResource* (p. 778)		
UpdateReplicationCertificate [permission only]	Grants permission to update a replication certificate	Write	RecoveryInstanceResource* (p. 778)		
UpdateReplicationConfiguration	Grants permission to update replication configuration	Write	SourceServerResource* (p. 778)		
UpdateReplicationConfigurationTemplate	Grants permission to update replication configuration template	Write	ReplicationConfigurationTemplateResource* (p. 778)		

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 \(p. 770\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 778)

Resource types	ARN	Condition keys
RecoveryInstances	arn:\${Partition}:drs:\${Region}:\${{Account}}:recovery-instance/\${RecoveryInstanceID}	aws:ResourceTag/\${TagKey} (p. 778) drs:EC2InstanceARN (p. 778)
ReplicationConfigurations	arn:\${Partition}:drs:\${Region}:\${{Account}}/replication-configuration-template/\${ReplicationConfigurationTemplateID}	aws:ResourceTag/\${TagKey} (p. 778)
SourceServerResources	arn:\${Partition}:drs:\${Region}:\${{Account}}:source-server/\${SourceServerID}	aws:ResourceTag/\${TagKey} (p. 778)

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 [Available global condition 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	String

Actions, resources, and condition keys for Amazon Elastic File System

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

References:

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

Topics

- [Actions defined by Amazon Elastic File System \(p. 779\)](#)

- [Resource types defined by Amazon Elastic File System \(p. 783\)](#)
- [Condition keys for Amazon Elastic File System \(p. 783\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 783)		
ClientMount [permission only]	Grants permission to allow an NFS client read-access to a file system	Read	file-system* (p. 783)		
				elasticfilesystem:AccessPointArn (p. 783)	elasticfilesystem:AccessedViaMountTa
ClientRootAccess [permission only]	Grants permission to allow an NFS client root-access to a file system	Write	file-system* (p. 783)		
				elasticfilesystem:AccessPointArn (p. 783)	elasticfilesystem:AccessedViaMountTa
ClientWrite [permission only]	Grants permission to allow an NFS client write-access to a file system	Write	file-system* (p. 783)		
				elasticfilesystem:AccessPointArn (p. 783)	elasticfilesystem:AccessedViaMountTa
CreateAccessPoint	Grants permission to create an access point for the specified file system	Write	file-system* (p. 783)		
				aws:TagKeys (p. 783)	aws:RequestTag/\${TagKey} (p. 783)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateFileSystem	Grants permission to create a new, empty file system	Write		aws:RequestTag/ \${TagKey} (p. 783) aws:TagKeys (p. 783) elasticfilesystem:Encrypted (p. 783)	
CreateMountTarget	Grants permission to create a mount target for a file system	Write	file-system* (p. 783)		
CreateReplicationConfiguration	Grants permission to create a replication configuration	Write	file-system* (p. 783)		
CreateTags	Grants permission to create or overwrite tags associated with a file system; deprecated, see TagResource	Tagging	file-system* (p. 783)		
				aws:RequestTag/ \${TagKey} (p. 783)	aws:TagKeys (p. 783)
DeleteAccessPoint	Grants permission to delete the specified access point	Write	access-point* (p. 783)		
DeleteFileSystem	Grants permission to delete a file system, permanently severing access to its contents	Write	file-system* (p. 783)		
DeleteFileSystemPolicy	Grants permission to delete the resource-level policy for a file system	Permissions management	file-system* (p. 783)		
DeleteMountTarget	Grants permission to delete the specified mount target	Write	file-system* (p. 783)		
DeleteReplicationConfiguration	Grants permission to delete a replication configuration	Write	file-system* (p. 783)		
DeleteTags	Grants permission to delete the specified tags from a file system; deprecated, see UntagResource	Tagging	file-system* (p. 783)		
				aws:TagKeys (p. 783)	aws:RequestTag/ \${TagKey} (p. 783)
DescribeAccessPointDescriptions	Grants permission to view the descriptions of Amazon EFS access points	List	access-point (p. 783)		
			file-system (p. 783)		
DescribeAccountPreferences	Grants permission to view the preferences in effect for an account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeBackupPolicy	Grants permission to view the BackupPolicy object for an Amazon EFS file system	Read	file-system* (p. 783)		
DescribeFileSystemPolicy	Grants permission to view the resource-level policy for an Amazon EFS file system	Read	file-system (p. 783)		
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 (p. 783)		
DescribeLifecycleConfiguration	Grants permission to view the Lifecycle Configuration object for an Amazon EFS file system	Read	file-system* (p. 783)		
DescribeMountTargetSecurityGroups	Grants permission to view the security groups in effect for a mount target	Read			
DescribeMountTargets	Grants permission to view the descriptions of all mount targets, or a specific mount target, for a file system	Read	file-system* (p. 783)		
			access-point (p. 783)		
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 (p. 783)		
DescribeTags	Grants permission to view the tags associated with a file system	Read	file-system* (p. 783)		
ListTagsForResource	Grants permission to view the tags associated with the specified Amazon EFS resource	Read	access-point (p. 783)		
			file-system (p. 783)		
ModifyMountTargetSecurityGroups	Grants permission to modify the set of security groups in effect for a mount target	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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* (p. 783)		
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* (p. 783)		
PutLifecycleConfiguration	Grants permission to enable lifecycle management by creating a new LifecycleConfiguration object	Write	file-system* (p. 783)		
Restore [permission only]	Grants permission to start a restore job for a backup of a file system	Write	file-system* (p. 783)		
TagResource	Grants permission to create or overwrite tags associated with the specified Amazon EFS resource	Tagging	access-point (p. 783)		
			file-system (p. 783)		
				aws:RequestTag/\${TagKey} (p. 783)	
				aws:TagKeys (p. 783)	
UntagResource	Grants permission to delete the specified tags from an Amazon EFS resource	Tagging	access-point (p. 783)		
			file-system (p. 783)		
				aws:TagKeys (p. 783)	
UpdateFileSystem	Grants permission to update the throughput mode or the amount of provisioned throughput of an existing file system	Write	file-system* (p. 783)		

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 \(p. 779\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
file-system	<code>arn:\${Partition}:elasticfilesystem:\${Region}:\${Account}:file-system/\${FileSystemId}</code>	aws:ResourceTag/\${TagKey} (p. 783)
access-point	<code>arn:\${Partition}:elasticfilesystem:\${Region}:\${Account}:access-point/\${AccessPointId}</code>	aws:ResourceTag/\${TagKey} (p. 783)

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 [Available global condition 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	String
elasticfilesystem:AccessPointTargets	Filters access by whether the file system is accessed via mounting targets	Bool
elasticfilesystem:Encrypted	Filters access by whether users can create only encrypted or unencrypted file systems	Bool

Actions, resources, and condition keys for Amazon Elastic Inference

Amazon Elastic Inference (service prefix: `elastic-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 Amazon Elastic Inference \(p. 784\)](#)
- [Resource types defined by Amazon Elastic Inference \(p. 785\)](#)
- [Condition keys for Amazon Elastic Inference \(p. 785\)](#)

Actions defined by Amazon Elastic 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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 customer for connecting to Elastic Inference accelerator	Write	accelerator* (p. 785)		
DescribeAccelerator	Grants permission to describe the regions in which a given accelerator type or set of types is present in a given region	List			
DescribeAccelerators	Grants permission to describe the accelerator types available in a given region, as well as their characteristics, such as memory and throughput	List			
DescribeAcceleratorTags	Grants permission to describe information over a provided set of accelerators belonging to an account	List			
ListTagsForResource	Grants permission to list all tags on an Amazon RDS resource	Read			
TagResource	Grants permission to assign one or more tags (key-value pairs)	Tagging			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	to the specified QuickSight resource				
UntagResource	Grants permission to remove a tag or tags from a resource	Tagging			

Resource types defined by Amazon Elastic 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 \(p. 784\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
accelerator	<code>arn:\${Partition}:elastic-inference:\${Region}:\${Account}:elastic-inference-accelerator/\${AcceleratorId}</code>	

Condition keys for Amazon Elastic Inference

EI 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 [Available keys for conditions](#).

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 \(p. 785\)](#)
- [Resource types defined by Amazon Elastic Kubernetes Service \(p. 789\)](#)
- [Condition keys for Amazon Elastic Kubernetes Service \(p. 790\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AccessKubernetes [permission only]	Grants permission to view Kubernetes objects via AWS EKS console	Read	cluster* (p. 790)		
AssociateEncryption	Grants permission to associate encryption configuration to a cluster	Write	cluster* (p. 790)		
AssociateIdentity	Grants permission to associate an identity provider configuration to a cluster	Write	cluster* (p. 790)		
				aws:RequestTag/\${TagKey} (p. 790)	
				aws:TagKeys (p. 790)	
				eks:clientId (p. 790)	
				eks:issuerUrl (p. 790)	
CreateAddon	Grants permission to create an Amazon EKS add-on	Write	cluster* (p. 790)		
				aws:RequestTag/\${TagKey} (p. 790)	
				aws:TagKeys (p. 790)	
CreateCluster	Grants permission to create an Amazon EKS cluster	Write		aws:RequestTag/\${TagKey} (p. 790)	
				aws:TagKeys (p. 790)	
CreateFargateProfile	Grants permission to create an AWS Fargate profile	Write	cluster* (p. 790)		
				aws:RequestTag/\${TagKey} (p. 790)	
				aws:TagKeys (p. 790)	
CreateNodegroup	Grants permission to create an Amazon EKS Nodegroup	Write	cluster* (p. 790)		
				aws:RequestTag/\${TagKey} (p. 790)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys (p. 790)	
DeleteAddon	Grants permission to delete an Amazon EKS add-on	Write	addon* (p. 790)		
DeleteCluster	Grants permission to delete an Amazon EKS cluster	Write	cluster* (p. 790)		
DeleteFargateProfile	Grants permission to delete an AWS Fargate profile	Write	fargateprofile* (p. 790)		
DeleteNodegroup	Grants permission to delete an Amazon EKS Nodegroup	Write	nodegroup* (p. 790)		
DeregisterCluster	Grants permission to deregister an External cluster	Write	cluster* (p. 790)		
DescribeAddon	Grants permission to retrieve descriptive information about an Amazon EKS add-on	Read	addon* (p. 790)		
DescribeAddonVersion	Grants permission to retrieve descriptive version information about the add-ons that Amazon EKS Add-ons supports	Read			
DescribeCluster	Grants permission to retrieve descriptive information about an Amazon EKS cluster	Read	cluster* (p. 790)		
DescribeFargateProfile	Grants permission to retrieve descriptive information about an AWS Fargate profile associated with a cluster	Read	fargateprofile* (p. 790)		
DescribeIdentityProviderConfig	Grants permission to retrieve descriptive information about an Idp config associated with a cluster	Read	identityproviderconfig* (p. 790)		
DescribeNodegroup	Grants permission to retrieve descriptive information about an Amazon EKS nodegroup	Read	nodegroup* (p. 790)		
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* (p. 790) addon (p. 790) nodegroup (p. 790)		
DisassociateIdentityProviderConfig	Grants permission to delete an associated Idp config	Write	identityproviderconfig* (p. 790)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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* (p. 790)		
ListClusters	Grants permission to list the Amazon EKS clusters in your AWS account (in the specified or default region)	List			
ListFargateProfile	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* (p. 790)		
ListIdentityProviderConfig	Grants permission to list the Idp config in your AWS account (in the specified or default region) associated with a given cluster	List	cluster* (p. 790)		
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* (p. 790)		
ListTagsForResource	Grants permission to list tags for the specified resource	Read	addon (p. 790)		
			cluster (p. 790)		
			fargateprofile (p. 790)		
			identityproviderconfig (p. 790)		
			nodegroup (p. 790)		
ListUpdates	Grants permission to list the updates for a given Amazon EKS cluster/nodegroup/add-on (in the specified or default region)	List	cluster* (p. 790)		
			addon (p. 790)		
			nodegroup (p. 790)		
RegisterCluster	Grants permission to register an External cluster	Write		aws:RequestTag/\${TagKey} (p. 790)	
				aws:TagKeys (p. 790)	
TagResource	Grants permission to tag the specified resource	Tagging	addon (p. 790)		
			cluster (p. 790)		
			fargateprofile (p. 790)		
			identityproviderconfig (p. 790)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			nodegroup (p. 790)		
				aws:RequestTag/ \${TagKey} (p. 790)	
				aws:TagKeys (p. 790)	
UntagResource	Grants permission to untag the specified resource	Tagging	addon (p. 790)		
			cluster (p. 790)		
			fargateprofile (p. 790)		
			identityproviderconfig (p. 790)		
			nodegroup (p. 790)		
				aws:TagKeys (p. 790)	
UpdateAddon	Grants permission to update Amazon EKS add-on configurations, such as the VPC-CNI version	Write	addon* (p. 790)		
UpdateClusterConfig	Grants permission to update Amazon EKS cluster configurations (eg: API server endpoint access)	Write	cluster* (p. 790)		
UpdateClusterVersion	Grants permission to update the Kubernetes version of an Amazon EKS cluster	Write	cluster* (p. 790)		
UpdateNodegroupAddon	Grants permission to update Amazon EKS nodegroup configurations (eg: min/max/desired capacity or labels)	Write	nodegroup* (p. 790)		
UpdateNodegroupVersion	Grants permission to update the Kubernetes version of an Amazon EKS nodegroup	Write	nodegroup* (p. 790)		

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 \(p. 785\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 790)
nodegroup	arn:\${Partition}:eks:\${Region}: \${Account}:nodegroup/\${ClusterName}/ \${NodegroupName}/\${UUID}	aws:ResourceTag/ \${TagKey} (p. 790)
addon	arn:\${Partition}:eks:\${Region}: \${Account}:addon/\${ClusterName}/ \${AddonName}/\${UUID}	aws:ResourceTag/ \${TagKey} (p. 790)
fargateprofile	arn:\${Partition}:eks:\${Region}: \${Account}:fargateprofile/\${ClusterName}/ \${FargateProfileName}/\${UUID}	aws:ResourceTag/ \${TagKey} (p. 790)
identityproviderconfig	arn:\${Partition}:eks:\${Region}: \${Account}:identityproviderconfig/ \${ClusterName}/\${IdentityProviderType}/ \${IdentityProviderConfigName}/\${UUID}	aws:ResourceTag/ \${TagKey} (p. 790)

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 [Available global condition 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:clientId	Filters access by the clientId present in the associateIdentityProviderConfig request the user makes to the EKS service	String
eks:issuerUrl	Filters access by the issuerUrl present in the associateIdentityProviderConfig request the user makes to the EKS service	String

Actions, resources, and condition keys for Elastic Load Balancing

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 Elastic Load Balancing \(p. 791\)](#)
- [Resource types defined by Elastic Load Balancing \(p. 794\)](#)
- [Condition keys for Elastic Load Balancing \(p. 794\)](#)

Actions defined by 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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 the specified tags to the specified load balancer. Each load balancer can have a maximum of 10 tags	Tagging	loadbalancer* (p. 794)		
			aws:RequestTag/ \${TagKey} (p. 794)		
			aws:TagKeys (p. 794)		
ApplySecurityGroupsToLoadBalancer	Associates one or more security groups with your load balancer in a virtual private cloud (VPC)	Write	loadbalancer* (p. 794)		
AttachLoadBalancerListeners	Adds one or more subnets to the set of configured subnets for the specified load balancer	Write	loadbalancer* (p. 794)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ConfigureHealthCheckSettings	Specifies the health check settings to use when evaluating the health state of your backend instances	Write	loadbalancer* (p. 794)		
CreateAppCookieWithStickySession	Generates a stickiness policy with sticky session lifetimes that follow that of an application-generated cookie	Write	loadbalancer* (p. 794)		
CreateLBCookieStickinessPolicy	Generates a stickiness policy with sticky session lifetimes controlled by the lifetime of the browser (user-agent) or a specified expiration period	Write	loadbalancer* (p. 794)		
CreateLoadBalancer	Creates a load balancer	Write	loadbalancer (p. 794)		
				aws:RequestTag/\${TagKey} (p. 794)	
CreateLoadBalancerListener	Creates one or more listeners for the specified load balancer	Write	loadbalancer* (p. 794)		
CreateLoadBalancerPolicy	Creates a policy with the specified attributes for the specified load balancer	Write	loadbalancer* (p. 794)		
DeleteLoadBalancer	Deletes the specified load balancer	Write	loadbalancer* (p. 794)		
DeleteLoadBalancerListener	Deletes the specified listeners from the specified load balancer	Write	loadbalancer* (p. 794)		
DeleteLoadBalancerPolicy	Deletes the specified policy from the specified load balancer. This policy must not be enabled for any listeners	Write	loadbalancer* (p. 794)		
DeregisterInstancesFromLoadBalancer	Deregisters the specified instances from the specified load balancer	Write	loadbalancer* (p. 794)		
DescribeInstanceState	Describes the state of the specified instances with respect to the specified load balancer	Read			
DescribeLoadBalancer	Describes the attributes for the specified load balancer	Read			
DescribeLoadBalancerPolicies	Describes the specified policies	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeLoadBalancers	Describes the specified load balancers. If no load balancers are specified, the call describes all of your load balancers	Read			
DescribeLoadBalancers	Describes the specified the load balancers. If no load balancers are specified, the call describes all of your load balancers	List			
DescribeTags	Describes the tags associated with the specified load balancers	Read	loadbalancer* (p. 794)		
DetachLoadBalancers	Removes the specified subnets from the set of configured subnets for the load balancer	Write	loadbalancer* (p. 794)		
DisableAvailabilityZones	Removes the specified Availability Zones from the set of Availability Zones for the specified load balancer	Write	loadbalancer* (p. 794)		
EnableAvailabilityZones	Adds the specified Availability Zones to the set of Availability Zones for the specified load balancer	Write	loadbalancer* (p. 794)		
ModifyLoadBalancerAttributes	Modifies the attributes of the specified load balancer	Write	loadbalancer* (p. 794)		
RegisterInstances	Adds the specified instances to the specified load balancer	Write	loadbalancer* (p. 794)		
RemoveTags	Removes one or more tags from the specified load balancer	Tagging	loadbalancer* (p. 794)		
				aws:RequestTag/\${TagKey} (p. 794)	
				aws:TagKeys (p. 794)	
SetLoadBalancerCertificates	Sets the certificate that terminates SSL for the specified listener's SSL connections	Write	loadbalancer* (p. 794)		
SetLoadBalancerPolicies	Replaces 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* (p. 794)		
SetLoadBalancerPoliciesForListener	Replaces the current set of policies for the specified load balancer port with the specified set of policies	Write	loadbalancer* (p. 794)		

Resource types defined by 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 \(p. 791\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
<code>loadbalancer</code>	<code>arn:\${Partition}:elasticloadbalancing:\${Region}:\${Account}:loadbalancer/\${LoadBalancerName}</code>	<code>aws:ResourceTag/\${TagKey}</code> (p. 794) <code>elasticloadbalancing:ResourceTag/\${TagKey}</code> (p. 794)

Condition keys for Elastic Load Balancing

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	A key that is present in the request the user makes to the ELB service	String
<code>aws:ResourceTag/\${TagKey}</code>	Global tag key and value pair	String
<code>aws:TagKeys</code>	The list of all the tag key names associated with the resource in the request	String
<code>elasticloadbalancing:ResourceTag/</code>	The preface string for a tag key and value pair attached to a <code>ResourceTag</code> /	String
<code>elasticloadbalancing:ResourceTag/\${TagKey}</code>	A tag key and value pair	String

Actions, resources, and condition keys for Elastic Load Balancing V2

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 Elastic Load Balancing V2 \(p. 795\)](#)
- [Resource types defined by Elastic Load Balancing V2 \(p. 800\)](#)
- [Condition keys for Elastic Load Balancing V2 \(p. 800\)](#)

Actions defined by 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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddListenerCertificates	Adds the specified certificates to the specified secure listener	Write	listener/app* (p. 800)		
			listener/net* (p. 800)		
AddTags	Adds the specified tags to the specified load balancer. Each load balancer can have a maximum of 10 tags	Tagging	listener-rule/app (p. 800)		
			listener-rule/net (p. 800)		
			listener/app (p. 800)		
			listener/net (p. 800)		
			loadbalancer/app/ (p. 800)		
			loadbalancer/net/ (p. 800)		
			targetgroup (p. 800)		
				aws:RequestTag/\${TagKey} (p. 801)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys (p. 801)	
CreateListener	Creates a listener for the specified Application Load Balancer	Write	loadbalancer/app/ (p. 800)		
			loadbalancer/net/ (p. 800)		
				aws:RequestTag/\${TagKey} (p. 801) aws:TagKeys (p. 801)	
CreateLoadBalancer	Creates a load balancer	Write	loadbalancer/app/ (p. 800)		
			loadbalancer/net/ (p. 800)		
				aws:RequestTag/\${TagKey} (p. 801) aws:TagKeys (p. 801)	
CreateRule	Creates a rule for the specified listener	Write	listener/app* (p. 800)		
			listener/net* (p. 800)		
				aws:RequestTag/\${TagKey} (p. 801) aws:TagKeys (p. 801)	
CreateTargetGroup	Creates a target group	Write	targetgroup* (p. 800)		
				aws:RequestTag/\${TagKey} (p. 801)	
				aws:TagKeys (p. 801)	
DeleteListener	Deletes the specified listener	Write	listener/app* (p. 800)		
			listener/net* (p. 800)		
DeleteLoadBalancer	Deletes the specified load balancer	Write	loadbalancer/app/ (p. 800)		
			loadbalancer/net/ (p. 800)		
DeleteRule	Deletes the specified rule	Write	listener-rule/app* (p. 800)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			listener-rule/net* (p. 800)		
DeleteTargetGroup	Deletes the specified target group	Write	targetgroup* (p. 800)		
DeregisterTargets	Deregisters the specified targets from the specified target group	Write	targetgroup* (p. 800)		
DescribeAccountBalancing	Describes the Elastic Load Balancing resource limits for the AWS account	Read			
DescribeListenerCertificates	Describes the certificates for the specified secure listener	Read			
DescribeListeners	Describes the specified listeners or the listeners for the specified Application Load Balancer	Read			
DescribeLoadBalancers	Describes the attributes for the specified load balancer	Read			
DescribeLoadBalancers	Describes the specified the load balancers. If no load balancers are specified, the call describes all of your load balancers	Read			
DescribeRules	Describes the specified rules or the rules for the specified listener	Read			
DescribeSSLPolicies	Describes the specified policies or all policies used for SSL negotiation	Read			
DescribeTags	Describes the tags associated with the specified resource	Read	listener-rule/app (p. 800)		
			listener-rule/net (p. 800)		
			listener/app (p. 800)		
			listener/net (p. 800)		
			loadbalancer/app/ (p. 800)		
			loadbalancer/net/ (p. 800)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			targetgroup (p. 800)		
DescribeTargetGroups	Describes the attributes for the specified target group	Read			
DescribeTargetGroups	Describes the specified target groups or all of your target groups	Read			
DescribeTargetHealth	Describes the health of the specified targets or all of your targets	Read			
ModifyListener	Modifies the specified properties of the specified listener	Write	listener/app* (p. 800)		
			listener/net* (p. 800)		
ModifyLoadBalancerAttributes	Modifies the attributes of the specified load balancer	Write	loadbalancer/app/ (p. 800)		
			loadbalancer/net/ (p. 800)		
ModifyRule	Modifies the specified rule	Write	listener-rule/app* (p. 800)		
			listener-rule/net* (p. 800)		
ModifyTargetGroupHealthCheck	Modifies the health checks used when evaluating the health state of the targets in the specified target group	Write	targetgroup* (p. 800)		
ModifyTargetGroupCertificates	Modifies the specified attributes of the specified target group	Write	targetgroup* (p. 800)		
RegisterTargets	Registers the specified targets with the specified target group	Write	targetgroup* (p. 800)		
RemoveListenerCertificates	Removes the specified certificates of the specified secure listener	Write	listener/app* (p. 800)		
			listener/net* (p. 800)		
RemoveTags	Removes one or more tags from the specified load balancer	Tagging	listener-rule/app (p. 800)		

Service Authorization Reference
 Service Authorization Reference
 Elastic Load Balancing V2

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			listener-rule/net (p. 800)		
			listener/app (p. 800)		
			listener/net (p. 800)		
			loadbalancer/app/ (p. 800)		
			loadbalancer/net/ (p. 800)		
			targetgroup (p. 800)		
			aws:RequestTag/\${TagKey} (p. 801)		
			aws:TagKeys (p. 801)		
SetIpAddressType	Not found	Write	loadbalancer/app/ (p. 800)		
				loadbalancer/net/ (p. 800)	
SetRulePriorities	Sets the priorities of the specified rules	Write	listener-rule/app* (p. 800)		
				listener-rule/net* (p. 800)	
SetSecurityGroup	Associates the specified security groups with the specified load balancer	Write	loadbalancer/app/ (p. 800)		
				loadbalancer/net/ (p. 800)	
SetSubnets	Enables the Availability Zone for the specified subnets for the specified load balancer	Write	loadbalancer/app/ (p. 800)		
				loadbalancer/net/ (p. 800)	
SetWebAcl [permission only]	Gives WebAcl permission to WAF	Write			

Resource types defined by 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 \(p. 795\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
listener/app	arn:\${Partition}:elasticloadbalancing:\${Region}:\${Account}:listener/app/\${LoadBalancerName}/\${LoadBalancerId}/\${ListenerId}	aws:ResourceTag/\${TagKey} (p. 801) elasticloadbalancing:ResourceTag/\${TagKey} (p. 801)
listener-rule/app	arn:\${Partition}:elasticloadbalancing:\${Region}:\${Account}:listener-rule/app/\${LoadBalancerName}/\${LoadBalancerId}/\${ListenerId}/\${ListenerRuleId}	aws:ResourceTag/\${TagKey} (p. 801) elasticloadbalancing:ResourceTag/\${TagKey} (p. 801)
listener/net	arn:\${Partition}:elasticloadbalancing:\${Region}:\${Account}:listener/net/\${LoadBalancerName}/\${LoadBalancerId}/\${ListenerId}	aws:ResourceTag/\${TagKey} (p. 801) elasticloadbalancing:ResourceTag/\${TagKey} (p. 801)
listener-rule/net	arn:\${Partition}:elasticloadbalancing:\${Region}:\${Account}:listener-rule/net/\${LoadBalancerName}/\${LoadBalancerId}/\${ListenerId}/\${ListenerRuleId}	aws:ResourceTag/\${TagKey} (p. 801) elasticloadbalancing:ResourceTag/\${TagKey} (p. 801)
loadbalancer/app	arn:\${Partition}:elasticloadbalancing:\${Region}:\${Account}:loadbalancer/app/\${LoadBalancerName}/\${LoadBalancerId}	aws:ResourceTag/\${TagKey} (p. 801) elasticloadbalancing:ResourceTag/\${TagKey} (p. 801)
loadbalancer/net	arn:\${Partition}:elasticloadbalancing:\${Region}:\${Account}:loadbalancer/net/\${LoadBalancerName}/\${LoadBalancerId}	aws:ResourceTag/\${TagKey} (p. 801) elasticloadbalancing:ResourceTag/\${TagKey} (p. 801)
targetgroup	arn:\${Partition}:elasticloadbalancing:\${Region}:\${Account}:targetgroup/\${TargetGroupName}/\${TargetGroupId}	aws:ResourceTag/\${TagKey} (p. 801) elasticloadbalancing:ResourceTag/\${TagKey} (p. 801)

Condition keys for Elastic Load Balancing V2

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	A key that is present in the request the user makes to the ELB service	String
<code>aws:ResourceTag/\${TagKey}</code>	Global tag key and value pair	String
<code>aws:TagKeys</code>	The list of all the tag key names associated with the resource in the request	ArrayOfString
<code>elasticloadbalancing:ResourceTag/\${TagKey}</code>	A tag key and value pair	String

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 \(p. 801\)](#)
- [Resource types defined by Amazon Elastic MapReduce \(p. 808\)](#)
- [Condition keys for Amazon Elastic MapReduce \(p. 809\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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
<code>AddInstanceFleet</code>	Grants permission to add an instance fleet to a running cluster	Write	cluster* (p. 808)		
<code>AddInstanceGroups</code>	Grants permission to add instance groups to a running cluster	Write	cluster* (p. 808)		
<code>AddJobFlowSteps</code>	Grants permission to add new steps to a running cluster	Write	cluster* (p. 808)		
<code>AddTags</code>	Grants permission to add tags to an Amazon EMR resource	Tagging	cluster (p. 808)		
			editor (p. 809)		aws:RequestTag/\${TagKey} (p. 809)
					aws:TagKeys (p. 809)
					elasticmapreduce:RequestTag/\${TagKey} (p. 809)
<code>AttachEditor</code> [permission only]	Grants permission to attach an EMR notebook to a compute engine	Write	editor* (p. 809)		
<code>CancelSteps</code>	Grants permission to cancel a pending step or steps in a running cluster	Write	cluster* (p. 808)		
<code>CreateEditor</code> [permission only]	Grants permission to create an EMR notebook	Write	cluster* (p. 808)		
					aws:RequestTag/\${TagKey} (p. 809)
					aws:TagKeys (p. 809)
					elasticmapreduce:RequestTag/\${TagKey} (p. 809)
<code>CreatePersistentApplicationHistoryServer</code>	Grants permission to create a persistent application history server	Write	cluster* (p. 808)		
<code>CreateRepository</code> [permission only]	Grants permission to create an EMR notebook repository	Write			
<code>CreateSecurityConfiguration</code>	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} (p. 809) aws:TagKeys (p. 809) elasticmapreduce:RequestTag/ \${TagKey} (p. 809)	
CreateStudioPresignedUrl	Grants permission to launch an EMR Studio using IAM authentication mode	Write	studio* (p. 809)		
CreateStudioSessionMapping	Grants permission to create an EMR Studio session mapping	Write	studio* (p. 809)		
DeleteEditor [permission only]	Grants permission to delete an EMR notebook	Write	editor* (p. 809)		
DeleteRepository [permission only]	Grants permission to delete an EMR notebook repository	Write			
DeleteSecurityConfiguration	Grants permission to delete a security configuration	Write			
DeleteStudio	Grants permission to delete an EMR Studio	Write	studio* (p. 809)		
DeleteStudioSessionMapping	Grants permission to delete an EMR Studio session mapping	Write	studio* (p. 809)		
DeleteWorkspaceAccess [permission only]	Grants permission to block a user from opening a collaborative workspace	Permissions management	editor* (p. 809)		
DescribeCluster	Grants permission to get details about a cluster, including status, hardware and software configuration, VPC settings, and so on	Read	cluster* (p. 808)		
DescribeEditor [permission only]	Grants permission to view information about a notebook, including status, user, role, tags, location, and more	Read	editor* (p. 809)		

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* (p. 808)		
DescribeNotebookExecutionInfo	Grants permission to view information about a notebook execution	Read	notebook-execution* (p. 809)		
DescribePersistentAppHistory	Grants permission to describe persistent application history server	Read	cluster* (p. 808)		
DescribeReleaseInfo	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 security configuration	Read			
DescribeStep	Grants permission to get details about a cluster step	Read	cluster* (p. 808)		
DescribeStudio	Grants permission to view information about an EMR Studio	Read	studio* (p. 809)		
DetachEditor [permission only]	Grants permission to detach an EMR notebook from a compute engine	Write	editor* (p. 809)		
GetAutoTerminationPolicy	Grants permission to retrieve the auto-termination policy associated with a cluster	Read	cluster* (p. 808)		
GetBlockPublicAccess	Grants permission to retrieve the EMR block public access configuration for the AWS account in the Region	Read			
GetManagedScalingPolicy	Grants permission to retrieve the managed scaling policy associated with a cluster	Read	cluster* (p. 808)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetOnClusterApp <small>[permission only]</small>	Grants permission to get a presigned URL for an application history server running on the cluster	Write	cluster* (p. 808)		
GetPersistentApp <small>[permission only]</small>	Grants permission to get a presigned URL for a persistent application history server	Write	cluster* (p. 808)		
GetStudioSessionMapping	Grants permission to view information about an EMR Studio session mapping	Read	studio* (p. 809)		
LinkRepository <small>[permission only]</small>	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* (p. 808)		
ListClusters	Grants permission to get the status of accessible clusters	List			
ListEditors <small>[permission only]</small>	Grants permission to list summary information for accessible EMR notebooks	List			
ListInstanceFleets	Grants permission to get details of instance fleets in a cluster	Read	cluster* (p. 808)		
ListInstanceGroups	Grants permission to get details of instance groups in a cluster	Read	cluster* (p. 808)		
ListInstances	Grants permission to get details about the Amazon EC2 instances in a cluster	Read	cluster* (p. 808)		
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 <small>[permission only]</small>	Grants permission to list existing EMR notebook repositories	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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* (p. 808)		
ListStudioSessionMappings	Grants permission to list summary information about EMR Studio session mappings	List			
ListStudios	Grants permission to list summary information about EMR Studios	List			
ListWorkspaceAccessIdentities [permission only]	Grants permission to list identities that are granted access to a workspace	List	editor* (p. 809)		
ModifyCluster	Grants permission to change cluster settings such as number of steps that can be executed concurrently for a cluster	Write	cluster* (p. 808)		
ModifyInstanceFleet	Grants permission to change the target On-Demand and target Spot capacities for a instance fleet	Write	cluster* (p. 808)		
ModifyInstanceGroup	Grants permission to change the number and configuration of EC2 instances for an instance group	Write	cluster (p. 808)		
OpenEditorInConsole [permission only]	Grants permission to launch the Jupyter notebook editor for an EMR notebook from within the console	Write	cluster* (p. 808)		
			editor* (p. 809)		
PutAutoScalingPolicy	Grants permission to create or update an automatic scaling policy for a core instance group or task instance group	Write	cluster* (p. 808)		
PutAutoTerminationPolicy	Grants permission to create or update the auto-termination policy associated with a cluster	Write	cluster* (p. 808)		
PutBlockPublicAccess	Grants permission to create or update the EMR block public access configuration for the AWS account in the Region	Permissions management			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutManagedScalingPolicy	Grants permission to create or update the managed scaling policy associated with a cluster	Write	cluster* (p. 808)		
PutWorkspaceAccessIdentity [permission only]	Grants permission to allow an identity to open a collaborative workspace	Permissions management	editor* (p. 809)		
RemoveAutoScalingPolicy	Grants permission to remove an automatic scaling policy from an instance group	Write	cluster* (p. 808)		
RemoveAutoTerminationPolicy	Grants permission to remove the auto termination policy associated with a cluster	Write	cluster* (p. 808)		
RemoveManagedScalingPolicy	Grants permission to remove the managed scaling policy associated with a cluster	Write	cluster* (p. 808)		
RemoveTags	Grants permission to remove tags from an Amazon EMR resource	Tagging	cluster (p. 808)		
			editor (p. 809)		
			aws:TagKeys (p. 809)		
RunJobFlow	Grants permission to create and launch a cluster (job flow)	Write		aws:RequestTag/ \${TagKey} (p. 809)	
				aws:TagKeys (p. 809)	
					elasticmapreduce:RequestTag/ \${TagKey} (p. 809)
SetTerminationProtection	Grants permission to add and remove termination protection for a cluster	Write	cluster* (p. 808)		
StartEditor [permission only]	Grants permission to start an EMR notebook	Write	cluster* (p. 808)		
			editor* (p. 809)		
StartNotebookExecution	Grants permission to start an EMR notebook execution	Write	cluster* (p. 808)		
			editor* (p. 809)		
					aws:RequestTag/ \${TagKey} (p. 809)
				aws:TagKeys (p. 809)	
					elasticmapreduce:RequestTag/ \${TagKey} (p. 809)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopEditor [permission only]	Grants permission to shut down an EMR notebook	Write	editor* (p. 809)		
StopNotebookExecution	Grants permission to stop notebook execution	Write	notebook-execution* (p. 809)		
TerminateJobFlow	Grants permission to terminate a cluster (job flow)	Write	cluster* (p. 808)		
UnlinkRepository [permission only]	Grants permission to unlink an EMR notebook repository from EMR notebooks	Write			
UpdateEditor [permission only]	Grants permission to update an EMR notebook	Write	editor* (p. 809)		
UpdateRepository [permission only]	Grants permission to update an EMR notebook repository	Write			
UpdateStudio	Grants permission to update information about an EMR Studio	Write	studio* (p. 809)		
UpdateStudioSession	Grants permission to update an EMR Studio session mapping	Write	studio* (p. 809)		
ViewEventsFromClusters [permission only]	Grants permission to use the ViewEventsFromClusters API 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 \(p. 801\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 809) elasticmapreduce:ResourceTag/\${TagKey} (p. 809)

Resource types	ARN	Condition keys
editor	arn:\${Partition}:elasticmapreduce:\${Region}:\${Account}:editor/\${EditorId}	aws:ResourceTag/\${TagKey} (p. 809) elasticmapreduce:ResourceTag/\${TagKey} (p. 809)
notebook-execution	arn:\${Partition}:elasticmapreduce:\${Region}:\${Account}:notebook-execution/\${NotebookExecutionId}	aws:ResourceTag/\${TagKey} (p. 809) elasticmapreduce:ResourceTag/\${TagKey} (p. 809)
studio	arn:\${Partition}:elasticmapreduce:\${Region}:\${Account}:studio/\${StudioId}	aws:ResourceTag/\${TagKey} (p. 809) elasticmapreduce:ResourceTag/\${TagKey} (p. 809)

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 [Available global condition 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:RequestWithTheAction\${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 \(p. 810\)](#)
- [Resource types defined by Amazon Elastic Transcoder \(p. 811\)](#)
- [Condition keys for Amazon Elastic Transcoder \(p. 812\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 811)		
CreateJob	Create a job.	Write	pipeline* (p. 811)		
			preset* (p. 811)		
CreatePipeline	Create a pipeline	Write	pipeline* (p. 811)		
CreatePreset	Create a preset.	Write	preset* (p. 811)		
DeletePipeline	Delete a pipeline	Write	pipeline* (p. 811)		
DeletePreset	Delete a preset	Write	preset* (p. 811)		
ListJobsByPipeline	Get a list of the jobs that you assigned to a pipeline	List	pipeline* (p. 811)		
ListJobsByStatus	Get information about all of the jobs associated with the current AWS account that have a specified status	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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* (p. 811)		
ReadPipeline	Get detailed information about a pipeline	Read	pipeline* (p. 811)		
ReadPreset	Get detailed information about a preset.	Read	preset* (p. 811)		
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* (p. 811)		
UpdatePipelineNotification	Update only Amazon Simple Notification Service (Amazon SNS) notifications for a pipeline	Write	pipeline* (p. 811)		
UpdatePipelineStatus	Pause or reactivate a pipeline, stop the pipeline stops or restarts processing jobs, update the status for the pipeline.	Write	pipeline* (p. 811)		

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 \(p. 810\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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 [Available keys for conditions](#).

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 \(p. 812\)](#)
- [Resource types defined by Amazon ElastiCache \(p. 825\)](#)
- [Condition keys for Amazon ElastiCache \(p. 828\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 (p. 827) parametergroup (p. 825)		

Service Authorization Reference
Service Authorization Reference
Amazon ElastiCache

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			replicationgroup (p. 826) reserved-instance (p. 827) securitygroup (p. 825) snapshot (p. 827) subnetgroup (p. 826) user (p. 828) usergroup (p. 828)		
AuthorizeCacheSecurityGroup	Grants permission to authorize an EC2 security group on a ElastiCache security group	Write	securitygroup* (p. 825) aws:ResourceTag/\${TagKey} (p. 829)	ec2:AuthorizeSecurityGroup	
BatchApplyUpdates	Grants permission to apply ElastiCache service updates to sets of clusters and replication groups	Write	cluster (p. 827) aws:RequestTag/\${TagKey} (p. 829)	ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs s3:GetObject	
BatchStopUpdates	Grants permission to stop ElastiCache service updates from being executed on a set of clusters	Write	cluster (p. 827) replicationgroup (p. 826) aws:ResourceTag/\${TagKey} (p. 829)		
CompleteMigration	Grants permission to complete an online migration of data from hosted Redis on Amazon EC2 to ElastiCache	Write	cluster (p. 827) replicationgroup (p. 826) aws:ResourceTag/\${TagKey} (p. 829)		

Service Authorization Reference
Service Authorization Reference
Amazon ElastiCache

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CopySnapshot	Grants permission to make a copy of an existing snapshot	Write	snapshot* (p. 827)		elasticache:AddTagsToResource s3:DeleteObject s3:GetBucketAcl s3:PutObject
CreateCacheCluster	Grants permission to create a cache cluster	Write	parametergroup* (p. 825) cluster (p. 827) aws:RequestTag/\${TagKey} (p. 829) aws:TagKeys (p. 829)		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs elasticache:AddTagsToResource s3:GetObject aws:RequestTag/ \${TagKey} (p. 829) aws:TagKeys (p. 829) elasticache:CacheNodeType (p. 829) elasticache:EngineVersion (p. 829) elasticache:EngineType (p. 829) elasticache:MultiAZEnabled (p. 829) elasticache:AuthTokenEnabled (p. 829) elasticache:SnapshotRetentionLimit (p. 829) elasticache:CacheParameterGroupName (p. 829)

Service Authorization Reference
Service Authorization Reference
Amazon ElastiCache

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			replicationgroup* (p. 826) elasticache:CacheNodeType (p. 829) elasticache:EngineVersion (p. 829) elasticache:EngineType (p. 829) elasticache:MultiAZEnabled (p. 829) elasticache:AuthTokenEnabled (p. 829) elasticache:SnapshotRetentionLimit (p. 829) elasticache:CacheParameterGroupName (p. 829)	securitygroup (p. 825)	
	Grants permission to create a parameter group	Write	parametergroup* (p. 825)	elasticache:AddTagsToReplicationGroup (p. 829)	
				aws:ResourceTag/\${TagKey} (p. 829) aws:RequestTag/\${TagKey} (p. 829) aws:TagKeys (p. 829)	elasticache:CacheParameterGroupName (p. 829)
	Grants permission to create a security group	Write	securitygroup* (p. 825)	elasticache:AddTagsToReplicationGroup (p. 829)	
				aws:ResourceTag/\${TagKey} (p. 829) aws:RequestTag/\${TagKey} (p. 829) aws:TagKeys (p. 829)	
	Grants permission to create a subnet group	Write	subnetgroup* (p. 826)	elasticache:AddTagsToReplicationGroup (p. 829)	
				aws:ResourceTag/\${TagKey} (p. 829) aws:RequestTag/\${TagKey} (p. 829) aws:TagKeys (p. 829)	
	Grants permission to create a global replication group	Write	globalreplicationgroup* (p. 828)		

Service Authorization Reference
Service Authorization Reference
Amazon ElastiCache

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			replicationgroup* (p. 826)		
CreateReplicationGroup	Grants permission to create a replication group	Write	parametergroup* (p. 825) cluster (p. 827) globalreplicagroup (p. 828)	ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs elasticache:AddTagsToResource s3:GetObject	elasticache:CacheParameterGroupName (p. 829) elasticache:CacheNodeType (p. 829) elasticache:ReplicasPerNodeGroup (p. 829) elasticache:EngineVersion (p. 829) elasticache:EngineType (p. 829) elasticache:AtRestEncryptionEnabled (p. 829) elasticache:TransitEncryptionEnabled (p. 829) elasticache:AutomaticFailoverEnabled (p. 829) elasticache:MultiAZEnabled (p. 829) elasticache:ClusterModeEnabled (p. 829) elasticache:AuthTokenEnabled (p. 829) elasticache:SnapshotRetentionLimit (p. 829) elasticache:KmsKeyId (p. 829) elasticache:CacheParameterGroupName (p. 829)

Service Authorization Reference
Service Authorization Reference
Amazon ElastiCache

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			replicationgroup (p. 826) aws:ResourceTag/ \${TagKey} (p. 829) aws:TagKeys (p. 829) elasticache:NumNodeGroups (p. 829) elasticache:CacheNodeType (p. 829) elasticache:ReplicasPerNodeGroup (p. 829) elasticache:EngineVersion (p. 829) elasticache:EngineType (p. 829) elasticache:AtRestEncryptionEnabled (p. 829) elasticache:TransitEncryptionEnabled (p. 829) elasticache:AutomaticFailoverEnabled (p. 829) elasticache:MultiAZEnabled (p. 829) elasticache:ClusterModeEnabled (p. 829) elasticache:AuthTokenEnabled (p. 829) elasticache:SnapshotRetentionLimit (p. 829) elasticache:KmsKeyId (p. 829) elasticache:CacheParameterGroupName (p. 829)	aws:ResourceTag/ \${TagKey} (p. 829) aws:TagKeys (p. 829) elasticache:NumNodeGroups (p. 829) elasticache:CacheNodeType (p. 829) elasticache:ReplicasPerNodeGroup (p. 829) elasticache:EngineVersion (p. 829) elasticache:EngineType (p. 829) elasticache:AtRestEncryptionEnabled (p. 829) elasticache:TransitEncryptionEnabled (p. 829) elasticache:AutomaticFailoverEnabled (p. 829) elasticache:MultiAZEnabled (p. 829) elasticache:ClusterModeEnabled (p. 829) elasticache:AuthTokenEnabled (p. 829) elasticache:SnapshotRetentionLimit (p. 829) elasticache:KmsKeyId (p. 829) elasticache:CacheParameterGroupName (p. 829)	aws:ResourceTag/ \${TagKey} (p. 829) aws:TagKeys (p. 829) elasticache:NumNodeGroups (p. 829) elasticache:CacheNodeType (p. 829) elasticache:ReplicasPerNodeGroup (p. 829) elasticache:EngineVersion (p. 829) elasticache:EngineType (p. 829) elasticache:AtRestEncryptionEnabled (p. 829) elasticache:TransitEncryptionEnabled (p. 829) elasticache:AutomaticFailoverEnabled (p. 829) elasticache:MultiAZEnabled (p. 829) elasticache:ClusterModeEnabled (p. 829) elasticache:AuthTokenEnabled (p. 829) elasticache:SnapshotRetentionLimit (p. 829) elasticache:KmsKeyId (p. 829) elasticache:CacheParameterGroupName (p. 829)
CreateSnapshot	Grants permission to create a copy of an entire Redis cluster at a specific moment in time	Write	snapshot* (p. 827) RequestTags (p. 827) aws:ResourceTag/ \${TagKey} (p. 829) aws:TagKeys (p. 829) elasticache:KmsKeyId (p. 829) s3:DeleteObject s3:GetBucketAcl s3:PutObject	aws:ResourceTag/ \${TagKey} (p. 829) aws:TagKeys (p. 829) elasticache:KmsKeyId (p. 829) s3:DeleteObject s3:GetBucketAcl s3:PutObject	aws:ResourceTag/ \${TagKey} (p. 829) aws:TagKeys (p. 829) elasticache:KmsKeyId (p. 829) s3:DeleteObject s3:GetBucketAcl s3:PutObject

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/ \${TagKey} (p. 829)	
CreateUser	Grants permission to create a Redis user for Redis engine version 6.x and onwards	Write	user* (p. 828) aws:RequestTag/ \${TagKey} (p. 829) aws:TagKeys (p. 829)	elasticache:AddTagsToRe	
CreateUserGroup	Grants permission to create a Redis user group for Redis engine version 6.x and onwards	Write	user* (p. 828) usergroup* (p. 828) aws:RequestTag/ \${TagKey} (p. 829) aws:TagKeys (p. 829) aws:ResourceTag/ \${TagKey} (p. 829)	elasticache:AddTagsToRe	
DecreaseNodeGroups	Grants permission to decrease the number of node groups in global replication groups	Write	globalreplicationgroup* (p. 828) elasticache:NumNodeGroups (p. 829)		
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* (p. 826) aws:ResourceTag/ \${TagKey} (p. 829) elasticache:ReplicasPerNodeGroup (p.	ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs	
DeleteCacheCluster	Grants permission to delete a previously provisioned cluster	Write	cluster* (p. 827) aws:ResourceTag/ \${TagKey} (p. 829) ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs snapshot (p. 827)	ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs	
DeleteCacheParameterGroup	Grants permission to delete the specified cache parameter group	Write	parametergroup* (p. 825)		

Service Authorization Reference
Service Authorization Reference
Amazon ElastiCache

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/ \${TagKey} (p. 829) elasticache:CacheParameterGroupName	
DeleteCacheSecurityGroup	Grants permission to delete a cache security group	Write	securitygroup*	(p. 825)	
				aws:ResourceTag/ \${TagKey} (p. 829)	
DeleteCacheSubnetGroup	Grants permission to delete a subnet group	Write	subnetgroup*	(p. 826)	ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/ \${TagKey} (p. 829)	
DeleteGlobalReplicationGroup	Grants permission to delete an existing global replication group	Write	globalreplicationgroup*	(p. 828)	
				aws:ResourceTag/ \${TagKey} (p. 829)	ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
DeleteReplicationGroup	Grants permission to delete an existing replication group	Write	replicationgroup*	(p. 826) aws:ResourceTag/ \${TagKey} (p. 829)	ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				snapshot (p. 827)	
DeleteSnapshot	Grants permission to delete an existing snapshot	Write	snapshot*	(p. 827)	
				aws:ResourceTag/ \${TagKey} (p. 829)	
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*	(p. 828)	
				aws:ResourceTag/ \${TagKey} (p. 829)	
DeleteUserGroup	Grants permission to delete an existing user group	Write	usergroup*	(p. 828)	
				aws:ResourceTag/ \${TagKey} (p. 829)	
DescribeCacheClusters	Grants permission to list information about provisioned cache clusters	List	cluster*	(p. 827)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/ \${TagKey} (p. 829)	
DescribeCacheEnginesAvailable	Grants permission to list available cache engines and their versions	List			
DescribeCacheParameterGroups	Grants permission to list cache parameter group descriptions	List	parametergroup* (p. 825)		
				aws:ResourceTag/ \${TagKey} (p. 829)	
DescribeCacheParameters	Grants permission to retrieve the detailed parameter list for a particular cache parameter group	List	parametergroup* (p. 825)		
				aws:ResourceTag/ \${TagKey} (p. 829)	
DescribeCacheSecurityGroups	Grants permission to list cache security group descriptions	List	securitygroup* (p. 825)		
				aws:ResourceTag/ \${TagKey} (p. 829)	
DescribeCacheSubnetGroups	Grants permission to list cache subnet group descriptions	List	subnetgroup* (p. 826)		
				aws:ResourceTag/ \${TagKey} (p. 829)	
DescribeEngineDefaults	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* (p. 828)		
DescribeReplicationGroups	Grants permission to list information about provisioned replication groups	List	replicationgroup* (p. 826)		
				aws:ResourceTag/ \${TagKey} (p. 829)	
DescribeReservedCacheNodes	Grants permission to list information about purchased reserved cache nodes	List	reserved-instance* (p. 827)		
				aws:ResourceTag/ \${TagKey} (p. 829)	
DescribeReservedCacheNodeOfferings	Grants permission to list available reserved cache node offerings	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeServiceUpdates	Grants permission to list details of the service updates	List			
DescribeSnapshotInfo	Grants permission to list information about cluster or replication group snapshots	List	snapshot* (p. 827) aws:ResourceTag/\${TagKey} (p. 829)		
DescribeUpdateActions	Grants permission to list details of the update actions for a set of clusters or replication groups	List	cluster (p. 827)		
			replicationgroup (p. 826)		
			aws:ResourceTag/\${TagKey} (p. 829)		
DescribeUserGroups	Grants permission to list information about Redis user groups	List	usergroup* (p. 828)		
			aws:ResourceTag/\${TagKey} (p. 829)		
DescribeUsers	Grants permission to list information about Redis users	List	user* (p. 828)		
			aws:ResourceTag/\${TagKey} (p. 829)		
DisassociateGlobalReplica	Grants permission to remove a secondary replication group from the global replication group	Write	globalreplicationgroup* (p. 828)		
FailoverGlobalReplica	Grants permission to failover the primary region to a selected secondary region of a global replication group	Write	globalreplicationgroup* (p. 828)		
IncreaseNodeGroups	Grants permission to increase the number of replica nodes in a global replication group	Write	globalreplicationgroup* (p. 828)		
			elasticache:NumNodeGroups (p. 829)		
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* (p. 826)	ec2:CreateNetworkInterface	
				ec2:DeleteNetworkInterface	
				ec2:DescribeNetworkInterfaces	
			aws:ResourceTag/\${TagKey} (p. 829)	ec2:DescribeSubnets	
				ec2:DescribeVpcs	
				elasticache:ReplicasPerNodeGroup (p. 829)	

Service Authorization Reference
Service Authorization Reference
Amazon ElastiCache

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAllowedNodeTypeAvailableNodes	Grants permission to list available node type that can be used to scale a particular Redis cluster or replication group	List	cluster (p. 827)		
	replicationgroup (p. 826)				
			aws:ResourceTag/\${TagKey} (p. 829)		
ListTagsForResource	Grants permission to list tags for an ElastiCache resource	Read	cluster (p. 827)		
	parametergroup (p. 825)				
	replicationgroup (p. 826)				
	reserved-instance (p. 827)				
	securitygroup (p. 825)				
	snapshot (p. 827)				
	subnetgroup (p. 826)				
	user (p. 828)				
	usergroup (p. 828)				
			aws:ResourceTag/\${TagKey} (p. 829)		
ModifyCacheCluster	Grants permission to modify settings for a cluster	Write	cluster* (p. 827)	elasticache:CacheNodeType (p. 829)	
	elasticache:EngineVersion (p. 829)				
	elasticache:MultiAZEnabled (p. 829)				
	elasticache:AuthTokenEnabled (p. 829)				
	elasticache:SnapshotRetentionLimit (p. 829)				
	elasticache:CacheParameterGroupName (p. 829)				
	parametergroup (p. 825)				
	securitygroup (p. 825)				
			aws:ResourceTag/\${TagKey} (p. 829)		
ModifyCacheParameterGroup	Grants permission to modify parameters of a cache parameter group	Write	parametergroup* (p. 825)		
			aws:ResourceTag/\${TagKey} (p. 829)		
			elasticache:CacheParameterGroupName (p. 829)		
ModifyCacheSubnetGroup	Grants permission to modify an existing cache subnet group	Write	subnetgroup* (p. 826)		

Service Authorization Reference
Service Authorization Reference
Amazon ElastiCache

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/\${TagKey} (p. 829)	
ModifyGlobalReplicationGroupSettings	Grants permission to modify global replication group settings for a global replication group	Write	globalreplicationgroup* (p. 828)		
ModifyReplicationGroupSettings	Grants permission to modify the settings for a replication group	Write	replicationgroup* (p. 826) ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs elasticache:SnapshotRetentionLimit (parametergroup (p. 825) securitygroup (p. 825) usergroup (p. 828))		
ModifyReplicationGroupShards	Grants permission to add shards, remove shards, or rebalance the keyspaces among existing shards of a replication group	Write	replicationgroup* (p. 826) ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs		
ModifyUser	Grants permission to change Redis user password(s) and/or access string	Write	user* (p. 828)		
ModifyUserGroup	Grants permission to change list of users that belong to the user group		aws:ResourceTag/\${TagKey} (p. 829) elasticache:NumNodeGroups (p. 829)		
			user* (p. 828)		
			usergroup* (p. 828)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/ \${TagKey} (p. 829)	
PurchaseReservedCacheOffering	Grants permission to purchase a reserved cache offering	Write	reserved-instance* (p. 827)		elasticache:AddTagsToReser...
				aws:ResourceTag/ \${TagKey} (p. 829)	
				aws:RequestTag/ \${TagKey} (p. 829)	
				aws:TagKeys (p. 829)	
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* (p. 828)		
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* (p. 827)		
				aws:ResourceTag/ \${TagKey} (p. 829)	
RemoveTagsFromResource	Grants permission to remove tags from a ElastiCache resource	Tagging	cluster (p. 827)		
			parametergroup (p. 825)		
			replicationgroup (p. 826)		
			reserved-instance (p. 827)		
			securitygroup (p. 825)		
			snapshot (p. 827)		
			subnetgroup (p. 826)		
			user (p. 828)		
			usergroup (p. 828)		
				aws:TagKeys (p. 829)	
				aws:ResourceTag/ \${TagKey} (p. 829)	
ResetCacheParameterGroup	Grants permission to modify parameters of a cache parameter group back to their default values	Write	parametergroup* (p. 825)		
				aws:ResourceTag/ \${TagKey} (p. 829)	
				elasticache:CacheParameterGroupNam...	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RevokeCacheSecurityGroup	Grants permission to remove an EC2 security group ingress from a ElastiCache security group	Write	securitygroup* (p. 825)		
				aws:ResourceTag/\${TagKey} (p. 829)	
StartMigration	Grants permission to start a migration of data from hosted Redis on Amazon EC2 to ElastiCache for Redis	Write	replicationgroup* (p. 826)		
				aws:ResourceTag/\${TagKey} (p. 829)	
TestFailover	Grants permission to test automatic failover on a specified node group in a replication group	Write	replicationgroup* (p. 826)	ec2:CreateNetworkInterface	
				ec2:DeleteNetworkInterface	
				ec2:DescribeNetworkInterface	
				ec2:DescribeSubnets	
				ec2:DescribeVpcs	
				aws:ResourceTag/\${TagKey} (p. 829)	

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 \(p. 812\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
parametergroup	<code>arn:\${Partition}:elasticache:\${Region}:\${Account}:parametergroup:\${CacheParameterGroupName}</code>	aws:RequestTag/\${TagKey} (p. 829) aws:ResourceTag/\${TagKey} (p. 829) aws:TagKeys (p. 829) elasticache:CacheParameterGroupName
securitygroup	<code>arn:\${Partition}:elasticache:\${Region}:\${Account}:securitygroup:\${CacheSecurityGroupName}</code>	aws:RequestTag/\${TagKey} (p. 829) aws:ResourceTag/\${TagKey} (p. 829) aws:TagKeys (p. 829)

Service Authorization Reference
Service Authorization Reference
Amazon ElastiCache

Resource types	ARN	Condition keys
subnetgroup	<code>arn:\${Partition}:elasticache:\${Region}:\${Account}:subnetgroup:\${CacheSubnetGroupName}</code>	aws:RequestTag/\${TagKey} (p. 829) aws:ResourceTag/\${TagKey} (p. 829) aws:TagKeys (p. 829)
replicationgroup	<code>arn:\${Partition}:elasticache:\${Region}:\${Account}:replicationgroup:\${ReplicationGroupId}</code>	aws:RequestTag/\${TagKey} (p. 829) aws:ResourceTag/\${TagKey} (p. 829) aws:TagKeys (p. 829) elasticache:AtRestEncryptionEnabled (p. 829) elasticache:AuthTokenEnabled (p. 829) elasticache:AutomaticFailoverEnabled (p. 829) elasticache:CacheNodeType (p. 829) elasticache:CacheParameterGroupName (p. 829) elasticache:ClusterModeEnabled (p. 829) elasticache:EngineType (p. 829) elasticache:EngineVersion (p. 829) elasticache:KmsKeyId (p. 829) elasticache:MultiAZEnabled (p. 829) elasticache:NumNodeGroups (p. 829) elasticache:ReplicasPerNodeGroup (p. 829) elasticache:SnapshotRetentionLimit (p. 829) elasticache:TransitEncryptionEnabled (p. 829)

Service Authorization Reference
Service Authorization Reference
Amazon ElastiCache

Resource types	ARN	Condition keys
cluster	<code>arn:\${Partition}:elasticache:\${Region}:\${Account}:cluster:\${CacheClusterId}</code>	aws:RequestTag/\${TagKey} (p. 829) aws:ResourceTag/\${TagKey} (p. 829) aws:TagKeys (p. 829) elasticache:AuthTokenEnabled (p. 829) elasticache:CacheNodeType (p. 829) elasticache:CacheParameterGroupName (p. 829) elasticache:EngineType (p. 829) elasticache:EngineVersion (p. 829) elasticache:MultiAZEnabled (p. 829) elasticache:SnapshotRetentionLimit (p. 829)
reserved-instance	<code>arn:\${Partition}:elasticache:\${Region}:\${Account}:reserved-instance:\${ReservedCacheNodeId}</code>	aws:RequestTag/\${TagKey} (p. 829) aws:ResourceTag/\${TagKey} (p. 829) aws:TagKeys (p. 829)
snapshot	<code>arn:\${Partition}:elasticache:\${Region}:\${Account}:snapshot:\${SnapshotName}</code>	aws:RequestTag/\${TagKey} (p. 829) aws:ResourceTag/\${TagKey} (p. 829) aws:TagKeys (p. 829) elasticache:KmsKeyId (p. 829)

Resource types	ARN	Condition keys
globalreplicationgroup	arn:\${Partition}:elasticache::\${Account}:globalreplicationgroup:\${GlobalReplicationGroupId}	elasticache:AtRestEncryptionEnabled (p. 829) elasticache:AuthTokenEnabled (p. 829) elasticache:AutomaticFailoverEnabled elasticache:CacheNodeType (p. 829) elasticache:CacheParameterGroupName elasticache:ClusterModeEnabled (p. 829) elasticache:EngineType (p. 829) elasticache:EngineVersion (p. 829) elasticache:KmsKeyId (p. 829) elasticache:MultiAZEnabled (p. 829) elasticache:NumNodeGroups (p. 829) elasticache:ReplicasPerNodeGroup (p. 829) elasticache:SnapshotRetentionLimit (p. 829) elasticache:TransitEncryptionEnabled (p. 829)
user	arn:\${Partition}:elasticache:\${Region}:\${Account}:user:\${UserId}	aws:RequestTag/\${TagKey} (p. 829) aws:ResourceTag/\${TagKey} (p. 829) aws:TagKeys (p. 829)
usergroup	arn:\${Partition}:elasticache:\${Region}:\${Account}:usergroup:\${UserGroupId}	aws:RequestTag/\${TagKey} (p. 829) aws:ResourceTag/\${TagKey} (p. 829) aws:TagKeys (p. 829)

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 [Available global condition keys](#).

Note

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
<code>aws:RequestTag/\${TagKey}</code>	Filters actions based on the tags that are passed in the request	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters actions based on the tags associated with the resource	String
<code>aws:TagKeys</code>	Filters actions based on the tag keys that are passed in the request	ArrayOfString
<code>elasticache:AtRestEncryptionEnabled</code>	Filters access by the AtRestEncryptionEnabled parameter present in the request or default false value if parameter is not present	Bool
<code>elasticache:AuthTokenParameter</code>	Filters access by the presence of non empty AuthToken parameter in the request	Bool
<code>elasticache:AutomaticFailoverEnabled</code>	Filters access by the AutomaticFailoverEnabled parameter in the request	Bool
<code>elasticache:CacheNodeType</code>	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
<code>elasticache:CacheParameterGroupName</code>	Filters access by the CacheParameterGroupName parameter in the request	String
<code>elasticache:ClusterMode</code>	Filters access by the cluster mode parameter present in the request. Default value for single node group (shard) creations is false	Bool
<code>elasticache:EngineType</code>	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
<code>elasticache:EngineVersion</code>	Filters access by the engineVersion parameter present in creation or cluster modification requests	String
<code>elasticache:KmsKeyId</code>	Filters access by the KmsKeyId parameter in the request	String
<code>elasticache:MultiAZEnabled</code>	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
<code>elasticache:NumNodeGroups</code>	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
<code>elasticache:ReplicasPerShard</code>	Filters access by the number of replicas per node group (shards) specified in creations or scaling requests	Numeric
<code>elasticache:SnapshotRetentionLimit</code>	Filters access by the SnapshotRetentionLimit parameter in the request	Numeric

Condition keys	Description	Type
<code>elasticache:TransitEncryptionInTheRequest</code>	Filters access by the <code>TransitEncryptionEnabled</code> parameter present in the request or default false value if parameter is not present	Bool

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 \(p. 830\)](#)
- [Resource types defined by AWS Elemental Appliances and Software \(p. 831\)](#)
- [Condition keys for AWS Elemental Appliances and Software \(p. 831\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateQuote [permission only]	Grants permission to create a quote	Tagging	quote* (p. 831)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys (p. 832)	
GetQuote [permission only]	Grants permission to describe a quote	Read	quote* (p. 831)		
ListQuotes [permission only]	Grants permission to list the quotes in the user account	List			
ListTagsForResource [permission only]	Grants permission to lists tags for an AWS Elemental Appliances and Software resource	Read	quote (p. 831)		
TagResource [permission only]	Grants permission to tag an AWS Elemental Appliances and Software resource	Tagging	quote (p. 831)		
				aws:TagKeys (p. 832)	
UntagResource [permission only]	Grants permission to remove a tag from an AWS Elemental Appliances and Software resource	Tagging	quote (p. 831)		
				aws:TagKeys (p. 832)	
UpdateQuote [permission only]	Grants permission to modify a quote	Write	quote* (p. 831)		

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 \(p. 830\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
quote	<code>arn:\${Partition}:elemental-appliances-software:\${Region}:\${Account}:quote/\${ResourceId}</code>	aws:ResourceTag/ \${TagKey} (p. 832)

Condition keys for AWS Elemental Appliances and Software

AWS Elemental Appliances and Software defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under

which the policy statement applies. For details about the columns in the following table, see [Condition keys table](#).

To view the global condition keys that are available to all services, see [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters access by request tag	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters access by resource tag	String
<code>aws:TagKeys</code>	Filters access by tag keys	ArrayOfString

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 \(p. 832\)](#)
- [Resource types defined by AWS Elemental Appliances and Software Activation Service \(p. 834\)](#)
- [Condition keys for AWS Elemental Appliances and Software Activation Service \(p. 834\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CompleteAccount [permission only]	Grants permission to complete the process of registering customer account for AWS Elemental Appliances and Software Purchases	Read			
CompleteFileUpload [permission only]	Grants permission to complete the process of uploading a Software file 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			
GenerateLicenses [permission only]	Grants permission to generate Software Licenses for AWS Elemental Appliances and Software Purchases	Read			
GetActivation [permission only]	Grants permission to describe an activation	Read	activation* (p. 834)		
ListTagsForResource [permission only]	Grants permission to list tags for an AWS Elemental Activations resource	Read	activation (p. 834)		
StartAccountRegistration [permission only]	Grants permission to start the process of registering customer account for AWS Elemental Appliances and Software Purchases	Read			
StartFileUpload [permission only]	Grants permission to start the process of uploading a Software file for AWS Elemental Appliances and Software Purchases	Read			
TagResource [permission only]	Grants permission to add a tag for an AWS Elemental Activations resource	Tagging	activation (p. 834)		
			aws:TagKeys (p. 834)	aws:RequestTag/\${TagKey} (p. 834)	
UntagResource	Grants permission to remove a tag from an AWS Elemental Activations resource	Tagging	activation (p. 834)		
			aws:TagKeys (p. 834)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
[permission only]					

Resource types defined by AWS Elemental Appliances and Software Activation 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 \(p. 832\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
activation	arn:\${Partition}:elemental-activations:\${Region}:\${Account}:activation/\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 834)

Condition keys for AWS Elemental Appliances and Software Activation Service

AWS Elemental Appliances and Software Activation 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 [Available global condition 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 \(p. 835\)](#)
- [Resource types defined by AWS Elemental MediaConnect \(p. 837\)](#)
- [Condition keys for AWS Elemental MediaConnect \(p. 837\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddFlowMediaStreams	Grants permission to add media streams to any flow	Write			
AddFlowOutputs	Grants permission to add outputs to any flow	Write			
AddFlowSources	Grants permission to add sources to any flow	Write			
AddFlowVpcInterfaces	Grants permission to add VPC interfaces to any flow	Write			
CreateFlow	Grants permission to create flows	Write			
DeleteFlow	Grants permission to delete flows	Write			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeOffering	Grants permission to display the details of an offering	Read			
DescribeReservation	Grants permission to display the details of a reservation	Read			
GrantFlowEntitlement	Grants permission to grant entitlements on any flow	Write			
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			
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			
ListTagsForResource	Grants permission to display a list of all tags associated with a resource	Read			
PurchaseOffering	Grants permission to purchase an offering	Write			
RemoveFlowMediaStreams	Grants permission to remove media streams from any flow	Write			
RemoveFlowOutputs	Grants permission to remove outputs from any flow	Write			
RemoveFlowSources	Grants permission to remove sources from any flow	Write			
RemoveFlowVpcInterfaces	Grants permission to remove VPC interfaces from any flow	Write			
RevokeFlowEntitlement	Grants permission to revoke entitlements on any flow	Write			
StartFlow	Grants permission to start flows	Write			
StopFlow	Grants permission to stop flows	Write			
TagResource	Grants permission to associate tags with resources	Tagging			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagResource	Grants permission to remove tags from resources	Tagging			
UpdateFlow	Grants permission to update flows	Write			
UpdateFlowEntitlement	Grants permission to update entitlements on any flow	Write			
UpdateFlowMediaStreams	Grants permission to update media streams on any flow	Write			
UpdateFlowOutputs	Grants permission to update outputs on any flow	Write			
UpdateFlowSources	Grants permission to update the source of any flow	Write			

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 \(p. 835\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
Entitlement	arn:\${Partition}:mediaconnect:\${Region}: \${Account}:entitlement:\${FlowId}: \${EntitlementName}	
Flow	arn:\${Partition}:mediaconnect:\${Region}: \${Account}:flow:\${FlowId}: \${FlowName}	
Output	arn:\${Partition}:mediaconnect:\${Region}: \${Account}:output:\${OutputId}: \${OutputName}	
Source	arn:\${Partition}:mediaconnect:\${Region}: \${Account}:source:\${SourceId}: \${SourceName}	

Condition keys for AWS Elemental MediaConnect

MediaConnect 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 [Available keys for conditions](#).

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 \(p. 838\)](#)
- [Resource types defined by AWS Elemental MediaConvert \(p. 841\)](#)
- [Condition keys for AWS Elemental MediaConvert \(p. 841\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateCertificate	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* (p. 841)		
CreateJob	Grants permission to create and submit an AWS Elemental MediaConvert job	Write	JobTemplate (p. 841)		
			Preset (p. 841)		
			Queue (p. 841)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 842) aws:TagKeys (p. 842)	
CreateJobTemplate	Grants permission to create an AWS Elemental MediaConvert custom job template	Write	Preset (p. 841)		
			Queue (p. 841)		
				aws:RequestTag/ \${TagKey} (p. 842) aws:TagKeys (p. 842)	
CreatePreset	Grants permission to create an AWS Elemental MediaConvert custom output preset	Write		aws:RequestTag/ \${TagKey} (p. 842) aws:TagKeys (p. 842)	
CreateQueue	Grants permission to create an AWS Elemental MediaConvert job queue	Write		aws:RequestTag/ \${TagKey} (p. 842) aws:TagKeys (p. 842)	
DeleteJobTemplate	Grants permission to delete an AWS Elemental MediaConvert custom job template	Write	JobTemplate* (p. 841)		
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* (p. 841)		
DeleteQueue	Grants permission to delete an AWS Elemental MediaConvert job queue	Write	Queue* (p. 841)		
DescribeEndpoint	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 the association between the Amazon Resource Name (ARN) of an AWS Certificate Manager (ACM) certificate and an AWS Elemental MediaConvert resource	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetJob	Grants permission to get an AWS Elemental MediaConvert job	Read	Job* (p. 841)		
GetJobTemplate	Grants permission to get an AWS Elemental MediaConvert job template	Read	JobTemplate* (p. 841)		
GetPolicy	Grants permission to get an AWS Elemental MediaConvert policy	Read			
GetPreset	Grants permission to get an AWS Elemental MediaConvert output preset	Read	Preset* (p. 841)		
GetQueue	Grants permission to get an AWS Elemental MediaConvert job queue	Read	Queue* (p. 841)		
ListJobTemplates	Grants permission to list AWS Elemental MediaConvert job templates	List			
ListJobs	Grants permission to list AWS Elemental MediaConvert jobs	List	Queue (p. 841)		
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	JobTemplate (p. 841)		
			Preset (p. 841)		
			Queue (p. 841)		
PutPolicy	Grants permission to put an AWS Elemental MediaConvert policy	Write			
TagResource	Grants permission to add tags to a MediaConvert queue, preset, or job template	Tagging	JobTemplate (p. 841)		
	Preset (p. 841)				
	Queue (p. 841)				
	aws:RequestTag/ {\$TagKey} (p. 842)				
UntagResource	Grants permission to remove tags from a MediaConvert queue, preset, or job template	Tagging	JobTemplate (p. 841)		
			Preset (p. 841)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Queue (p. 841) aws:TagKeys (p. 842)		
UpdateJobTemplate	Grants permission to update an AWS Elemental MediaConvert custom job template	Write	JobTemplate* (p. 841)		
			Preset (p. 841)		
			Queue (p. 841)		
UpdatePreset	Grants permission to update an AWS Elemental MediaConvert custom output preset	Write	Preset* (p. 841)		
UpdateQueue	Grants permission to update an AWS Elemental MediaConvert job queue	Write	Queue* (p. 841)		

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 \(p. 838\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 842)
Queue	arn:\${Partition}:mediaconvert:\${Region}: \${Account}:queues/\${QueueName}	aws:ResourceTag/ \${TagKey} (p. 842)
Preset	arn:\${Partition}:mediaconvert:\${Region}: \${Account}:presets/\${PresetName}	aws:ResourceTag/ \${TagKey} (p. 842)
JobTemplate	arn:\${Partition}:mediaconvert:\${Region}: \${Account}:jobTemplates/\${JobTemplateName}	aws:ResourceTag/ \${TagKey} (p. 842)
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 [Available global condition keys](#).

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

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 \(p. 842\)](#)
- [Resource types defined by AWS Elemental MediaLive \(p. 847\)](#)
- [Condition keys for AWS Elemental MediaLive \(p. 848\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
<code>AcceptInputDeviceTransfer</code>	Grants permission to accept an input device transfer	Write	input-device* (p. 847)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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* (p. 847)		
CancelInputDeviceTransfer	Grants permission to cancel an input device transfer	Write	input-device* (p. 847)		
ClaimDevice	Grants permission to claim an input device	Write	input-device* (p. 847)		
CreateChannel	Grants permission to create a channel	Write	channel* (p. 847)		
			input* (p. 847)		
			aws:RequestTag/ \${TagKey} (p. 848) aws:TagKeys (p. 848)		
CreateInput	Grants permission to create an input	Write	input* (p. 847)		
			input-security-group* (p. 847)		
			aws:RequestTag/ \${TagKey} (p. 848) aws:TagKeys (p. 848)		
CreateInputSecurityGroup	Grants permission to create an input security group	Write	input-security-group* (p. 847)		
			aws:RequestTag/ \${TagKey} (p. 848) aws:TagKeys (p. 848)		
			aws:RequestTag/ \${TagKey} (p. 848) aws:TagKeys (p. 848)		
CreateMultiplex	Grants permission to create a multiplex	Write	multiplex* (p. 847)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateMultiplexProgram	Grants permission to create a multiplex program	Write	multiplex* (p. 847)		
CreatePartnerInput	Grants permission to create a partner input	Write	input* (p. 847) aws:RequestTag/ {\$TagKey} (p. 848) aws:TagKeys (p. 848)		
CreateTags	Grants permission to create tags for channels, inputs, input security groups, multiplexes, and reservations	Tagging	channel (p. 847)		
			input (p. 847)		
			input-security-group (p. 847)		
			multiplex (p. 847)		
			reservation (p. 847)		
				aws:TagKeys (p. 848)	
				aws:RequestTag/ {\$TagKey} (p. 848)	
DeleteChannel	Grants permission to delete a channel	Write	channel* (p. 847)		
DeleteInput	Grants permission to delete an input	Write	input* (p. 847)		
DeleteInputSecurityGroup	Grants permission to delete an input security group	Write	input-security-group* (p. 847)		
DeleteMultiplex	Grants permission to delete a multiplex	Write	multiplex* (p. 847)		
DeleteMultiplexProgram	Grants permission to delete a multiplex program	Write	multiplex* (p. 847)		
DeleteReservation	Grants permission to delete an expired reservation	Write	reservation* (p. 847)		
DeleteSchedule	Grants permission to delete all schedule actions for a channel	Write	channel* (p. 847)		
DeleteTags	Grants permission to delete tags from channels, inputs, input security groups, multiplexes, and reservations	Tagging	channel (p. 847)		
			input (p. 847)		
			input-security-group (p. 847)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			multiplex (p. 847)		
			reservation (p. 847)		
				aws:TagKeys (p. 848)	
DescribeChannel	Grants permission to get details about a channel	Read	channel* (p. 847)		
DescribeInput	Grants permission to describe an input	Read	input* (p. 847)		
DescribeInputDevice	Grants permission to describe an input device	Read	input-device* (p. 847)		
DescribeInputDeviceThumbnail	Grants permission to describe an input device thumbnail	Read	input-device* (p. 847)		
DescribeInputSecurityGroup	Grants permission to describe an input security group	Read	input-security-group* (p. 847)		
DescribeMultiplex	Grants permission to describe a multiplex	Read	multiplex* (p. 847)		
DescribeMultiplexProgram	Grants permission to describe a multiplex program	Read	multiplex* (p. 847)		
DescribeOffering	Grants permission to get details about a reservation offering	Read	offering* (p. 847)		
DescribeReservation	Grants permission to get details about a reservation	Read	reservation* (p. 847)		
DescribeSchedule	Grants permission to view a list of actions scheduled on a channel	Read	channel* (p. 847)		
ListChannels	Grants permission to list channels	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			
ListMultiplexPrograms	Grants permission to list multiplex programs	List			
ListMultiplexes	Grants permission to list multiplexes	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListOfferings	Grants permission to list reservation offerings	List			
ListReservations	Grants permission to list reservations	List			
ListTagsForResource	Grants permission to list tags for channels, inputs, input security groups, multiplexes, and reservations	List	channel (p. 847)		
			input (p. 847)		
			input-security-group (p. 847)		
			multiplex (p. 847)		
			reservation (p. 847)		
PurchaseOffering	Grants permission to purchase a reservation offering	Write	offering* (p. 847)		
				reservation* (p. 847)	
				aws:RequestTag/ \${TagKey} (p. 848)	aws:TagKeys (p. 848)
RejectInputDeviceTransfer	Grants permission to reject an input device transfer	Write	input-device* (p. 847)		
StartChannel	Grants permission to start a channel	Write	channel* (p. 847)		
StartMultiplex	Grants permission to start a multiplex	Write	multiplex* (p. 847)		
StopChannel	Grants permission to stop a channel	Write	channel* (p. 847)		
StopMultiplex	Grants permission to stop a multiplex	Write	multiplex* (p. 847)		
TransferInputDevice	Grants permission to transfer an input device	Write	input-device* (p. 847)		
UpdateChannel	Grants permission to update a channel	Write	channel* (p. 847)		
UpdateChannelClass	Grants permission to update the class of a channel	Write	channel* (p. 847)		
UpdateInput	Grants permission to update an input	Write	input* (p. 847)		
UpdateInputDevice	Grants permission to update an input device	Write	input-device* (p. 847)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateInputSecurityGroup	Grants permission to update an input security group	Write	input-security-group* (p. 847)		
				aws:RequestTag/\${TagKey} (p. 848) aws:TagKeys (p. 848)	
UpdateMultiplex	Grants permission to update a multiplex	Write	multiplex* (p. 847)		
UpdateMultiplexProgram	Grants permission to update a multiplex program	Write	multiplex* (p. 847)		
UpdateReservation	Grants permission to update a reservation	Write	reservation* (p. 847)		

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 \(p. 842\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 848)
input	arn:\${Partition}:medialive:\${Region}: \${Account}:input:\${InputId}	aws:ResourceTag/\${TagKey} (p. 848)
input-device	arn:\${Partition}:medialive:\${Region}: \${Account}:inputDevice:\${DeviceId}	
input-security-group	arn:\${Partition}:medialive:\${Region}: \${Account}:inputSecurityGroup: \${InputSecurityGroupId}	aws:ResourceTag/\${TagKey} (p. 848)
multiplex	arn:\${Partition}:medialive:\${Region}: \${Account}:multiplex:\${MultiplexId}	aws:ResourceTag/\${TagKey} (p. 848)
reservation	arn:\${Partition}:medialive:\${Region}: \${Account}:reservation:\${ReservationId}	aws:ResourceTag/\${TagKey} (p. 848)
offering	arn:\${Partition}:medialive:\${Region}: \${Account}:offering:\${OfferingId}	

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters access by the tags that are passed in the request	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters access by the tags associated with the resource	String
<code>aws:TagKeys</code>	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 \(p. 848\)](#)
- [Resource types defined by AWS Elemental MediaPackage \(p. 850\)](#)
- [Condition keys for AWS Elemental MediaPackage \(p. 851\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 850)		iam:CreateServiceLinkedRole
CreateChannel	Grants permission to create a channel in AWS Elemental MediaPackage	Write		aws:RequestTag/\${TagKey} (p. 851) aws:TagKeys (p. 851)	
CreateHarvestJob	Grants permission to create a harvest job in AWS Elemental MediaPackage	Write		aws:RequestTag/\${TagKey} (p. 851) aws:TagKeys (p. 851)	
CreateOriginEndpoint	Grants permission to create an endpoint in AWS Elemental MediaPackage	Write		aws:RequestTag/\${TagKey} (p. 851) aws:TagKeys (p. 851)	
DeleteChannel	Grants permission to delete a channel in AWS Elemental MediaPackage	Write	channels* (p. 850)		
DeleteOriginEndpoint	Grants permission to delete an endpoint in AWS Elemental MediaPackage	Write	origin_endpoints* (p. 851)		
DescribeChannel	Grants permission to view the details of a channel in AWS Elemental MediaPackage	Read	channels* (p. 850)		
DescribeHarvestJob	Grants permission to view the details of a harvest job in AWS Elemental MediaPackage	Read	harvest_jobs* (p. 851)		
DescribeOriginEndpoint	Grants permission to view the details of an endpoint in AWS Elemental MediaPackage	Read	origin_endpoints* (p. 851)		
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 (p. 850) harvest_jobs (p. 851)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			origin_endpoints (p. 851)		
RotateChannelCredentials	Grants permission to rotate credentials for the first IngestEndpoint of a Channel in AWS Elemental MediaPackage	Write	channels* (p. 850)		
RotateIngestEndpointCredentials	Grants permission to rotate IngestEndpoint credentials for a Channel in AWS Elemental MediaPackage	Write	channels* (p. 850)		
TagResource	Grants permission to tag a MediaPackage resource	Tagging	channels (p. 850) harvest_jobs (p. 851) origin_endpoints (p. 851) aws:RequestTag/\${TagKey} (p. 851) aws:TagKeys (p. 851)		
UntagResource	Grants permission to delete tags to a Channel or OriginEndpoint	Tagging	channels (p. 850) harvest_jobs (p. 851) origin_endpoints (p. 851) aws:TagKeys (p. 851)		
UpdateChannel	Grants permission to make changes to a channel in AWS Elemental MediaPackage	Write	channels* (p. 850)		
UpdateOriginEndpoint	Grants permission to make changes to an endpoint in AWS Elemental MediaPackage	Write	origin_endpoints* (p. 851)		

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 \(p. 848\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
<code>channels</code>	<code>arn:\${Partition}:mediapackage:\${Region}:\${Account}:channels/\${ChannelIdentifier}</code>	<code>aws:ResourceTag/\${TagKey} (p. 851)</code>

Resource types	ARN	Condition keys
origin_endpoints	arn:\${Partition}:mediapackage:\${Region}:\${Account}:origin_endpoints/\${OriginEndpointIdentifier}	aws:ResourceTag/\${TagKey} (p. 851)
harvest_jobs	arn:\${Partition}:mediapackage:\${Region}:\${Account}:harvest_jobs/\${HarvestJobIdentifier}	aws:ResourceTag/\${TagKey} (p. 851)

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 [Available global condition 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 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 \(p. 851\)](#)
- [Resource types defined by AWS Elemental MediaPackage VOD \(p. 853\)](#)
- [Condition keys for AWS Elemental MediaPackage VOD \(p. 854\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the **Resource** element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 854)		iam:CreateServiceLinkedRole
CreateAsset	Grants permission to create an asset in AWS Elemental MediaPackage	Write		aws:RequestTag/\${TagKey} (p. 854) aws:TagKeys (p. 854)	
CreatePackagingConfiguration	Grants permission to create a packaging configuration in AWS Elemental MediaPackage	Write		aws:RequestTag/\${TagKey} (p. 854) aws:TagKeys (p. 854)	
CreatePackagingGroup	Grants permission to create a packaging group in AWS Elemental MediaPackage	Write		aws:RequestTag/\${TagKey} (p. 854) aws:TagKeys (p. 854)	
DeleteAsset	Grants permission to delete an asset in AWS Elemental MediaPackage	Write	assets* (p. 854)		
DeletePackagingConfiguration	Grants permission to delete a packaging configuration in AWS Elemental MediaPackage	Write	packaging-configurations* (p. 854)		
DeletePackagingGroup	Grants permission to delete a packaging group in AWS Elemental MediaPackage	Write	packaging-groups* (p. 854)		
DescribeAsset	Grants permission to view the details of an asset in AWS Elemental MediaPackage	Read	assets* (p. 854)		
DescribePackagingConfiguration	Grants permission to view the details of a packaging configuration in AWS Elemental MediaPackage	Read	packaging-configurations* (p. 854)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribePackagingGroups	Grants permission to view the details of a packaging group in AWS Elemental MediaPackage	Read	packaging-groups* (p. 854)		
ListAssets	Grants permission to view a list of assets in AWS Elemental MediaPackage	List			
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 PackagingGroup, PackagingConfiguration, or Asset	Read	assets (p. 854)		
			packaging-configurations (p. 854)		
			packaging-groups (p. 854)		
			aws:RequestTag / \${TagKey} (p. 854)		
TagResource	Grants permission to assign tags to a PackagingGroup, PackagingConfiguration, or Asset	Tagging	assets (p. 854)		
			packaging-configurations (p. 854)		
			packaging-groups (p. 854)		
			aws:TagKeys (p. 854)		
UntagResource	Grants permission to delete tags from a PackagingGroup, PackagingConfiguration, or Asset	Tagging	assets (p. 854)		
			packaging-configurations (p. 854)		
			packaging-groups (p. 854)		
			aws:TagKeys (p. 854)		
UpdatePackagingGroup	Grants permission to update a packaging group in AWS Elemental MediaPackage	Write	packaging-groups* (p. 854)		

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](#) (p. 851) identifies the resource

types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 854)
packaging-configurations	arn:\${Partition}:mediapackage-vod:\${Region}: \${Account}:packaging-configurations/ \${PackagingConfigurationIdentifier}	aws:ResourceTag/\${TagKey} (p. 854)
packaging-groups	arn:\${Partition}:mediapackage-vod: \${Region}: \${Account}:packaging-groups/ \${PackagingGroupIdentifier}	aws:ResourceTag/\${TagKey} (p. 854)

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 [Available global condition 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 \(p. 855\)](#)
- [Resource types defined by AWS Elemental MediaStore \(p. 857\)](#)

- Condition keys for AWS Elemental MediaStore (p. 857)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 (p. 857) aws:RequestTag/\${TagKey} (p. 857)	
DeleteContainer	Grants permission to delete a container	Write	container* (p. 857)		
DeleteContainerPolicy	Grants permission to delete the <code>Access</code> policy of a container	Permissions management	container* (p. 857)		
DeleteCorsPolicy	Grants permission to delete the CORS policy from a container	Write	container* (p. 857)		
DeleteLifecyclePolicy	Grants permission to delete the <code>Lifecycle</code> policy from a container	Write	container* (p. 857)		
DeleteMetricPolicy	Grants permission to delete the metric policy from a container	Write	container* (p. 857)		
DeleteObject	Grants permission to delete an object	Write	object* (p. 857)		
DescribeContainer	Grants permission to retrieve details on a container	List	container* (p. 857)		
DescribeObject	Grants permission to retrieve metadata for an object	List	object* (p. 857)		
GetContainerPolicy	Grants permission to retrieve the <code>Access</code> policy of a container	Read	container* (p. 857)		
GetCorsPolicy	Grants permission to retrieve the CORS policy of a container	Read	container* (p. 857)		

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* (p. 857)		
GetMetricPolicy	Grants permission to retrieve the metric policy that is assigned to a container	Read	container* (p. 857)		
GetObject	Grants permission to retrieve an object	Read	object* (p. 857)		
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 (p. 857)		
ListTagsForResource	Grants permission to list tags on a container	Read	container (p. 857)		
PutContainerPolicy	Grants permission to create or replace the access policy of a container	Permissions management	container* (p. 857)		
PutCorsPolicy	Grants permission to add or modify the CORS policy of a container	Write	container* (p. 857)		
PutLifecyclePolicy	Grants permission to add or modify the lifecycle policy that is assigned to a container	Write	container* (p. 857)		
PutMetricPolicy	Grants permission to add or modify the metric policy that is assigned to a container	Write	container* (p. 857)		
PutObject	Grants permission to upload an object	Write	object* (p. 857)		
StartAccessLogging	Grants permission to start access logging on a container	Write	container* (p. 857)		iam:PassRole
StopAccessLogging	Grants permission to stop access logging on a container	Write	container* (p. 857)		
TagResource	Grants permission to add tags to a container	Tagging	container (p. 857)		
				aws:TagKeys (p. 857)	
				aws:RequestTag/\${TagKey} (p. 857)	
UntagResource	Grants permission to remove tags from a container	Tagging	container (p. 857)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys (p. 857) aws:RequestTag/ {\$TagKey} (p. 857)	

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 \(p. 855\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 857)
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 [Available global condition 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	String

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 \(p. 858\)](#)
- [Resource types defined by AWS Elemental MediaTailor \(p. 862\)](#)
- [Condition keys for AWS Elemental MediaTailor \(p. 863\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ConfigureLogsForPlayback	Grants permission to configure logs for a playback configuration	Write	playbackConfiguration* (p. 863)		createServiceLinkedRole
CreateChannel	Grants permission to create a new channel	Write		aws:RequestTag/\${TagKey} (p. 863) aws:TagKeys (p. 863)	
CreateLiveSource	Grants permission to create a new live source on the source location with the specified source location name	Write	sourceLocation* (p. 863)		
				aws:RequestTag/\${TagKey} (p. 863) aws:TagKeys (p. 863)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePrefetchSchedule	Grants permission to create a prefetch schedule for the playback configuration with the specified playback configuration name	Write	playbackConfiguration* (p. 863)		
CreateProgram	Grants permission to create a new program on the channel with the specified channel name	Write	channel* (p. 863)		
CreateSourceLocation	Grants permission to create a new source location	Write		aws:RequestTag/\${TagKey} (p. 863) aws:TagKeys (p. 863)	
CreateVodSource	Grants permission to create a new VOD source on the source location with the specified source location name	Write	sourceLocation* (p. 863)		
DeleteChannel	Grants permission to delete the channel with the specified channel name	Write	channel* (p. 863)		
DeleteChannelPolicy	Grants permission to delete the IAM policy on the channel with the specified channel name	Permissions management	channel* (p. 863)		
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* (p. 863) sourceLocation* (p. 863)		
DeletePlaybackConfiguration	Grants permission to delete the specified playback configuration	Write	playbackConfiguration* (p. 863)		
DeletePrefetchSchedule	Grants permission to delete a prefetch schedule for a playback configuration with the specified prefetch schedule name	Write	playbackConfiguration* (p. 863) prefetchSchedule* (p. 863)		
DeleteProgram	Grants permission to delete the program with the specified program name on the channel with the specified channel name	Write	channel* (p. 863) program* (p. 863)		
DeleteSourceLocation	Grants permission to delete the source location with the specified source location name	Write	sourceLocation* (p. 863)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	sourceLocation* (p. 863)		
			vodSource* (p. 863)		
DescribeChannel	Grants permission to retrieve the channel with the specified channel name	Read	channel* (p. 863)		
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* (p. 863)		
			sourceLocation* (p. 863)		
DescribeProgram	Grants permission to retrieve the program with the specified program name on the channel with the specified channel name	Read	channel* (p. 863)		
			program* (p. 863)		
DescribeSourceLocation	Grants permission to retrieve the source location with the specified source location name	Read	sourceLocation* (p. 863)		
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	sourceLocation* (p. 863)		
			vodSource* (p. 863)		
GetChannelPolicy	Grants permission to read the IAM policy on the channel with the specified channel name	Read	channel* (p. 863)		
GetChannelSchedule	Grants permission to retrieve the schedule of programs on the channel with the specified channel name	Read	channel* (p. 863)		
GetPlaybackConfiguration	Grants permission to retrieve the configuration for the specified name	Read	playbackConfiguration* (p. 863)		
GetPrefetchSchedule	Grants permission to retrieve the prefetch schedule for a playback configuration with the specified prefetch schedule name	Read	playbackConfiguration* (p. 863)		
			prefetchSchedule* (p. 863)		
ListAlerts	Grants permission to retrieve the list of alerts on a resource	Read			
ListChannels	Grants permission to retrieve the list of existing channels	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListLiveSources	Grants permission to retrieve the list of existing live sources on the source location with the specified source location name	Read	sourceLocation* (p. 863)		
ListPlaybackConfigurations	Grants permission to retrieve the list of available configurations	List			
ListPrefetchSchedules	Grants permission to retrieve the list of prefetch schedules for a playback configuration	List	playbackConfiguration* (p. 863)		
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 (p. 863)		
			liveSource (p. 863)		
			playbackConfiguration (p. 863)		
			sourceLocation (p. 863)		
			vodSource (p. 863)		
ListVodSources	Grants permission to retrieve the list of existing VOD sources on the source location with the specified source location name	Read	sourceLocation* (p. 863)		
PutChannelPolicy	Grants permission to set the IAM policy on the channel with the specified channel name	Permissions management	channel* (p. 863)		
PutPlaybackConfiguration	Grants permission to add a new configuration		aws:RequestTag/ \${TagKey} (p. 863)		
StartChannel	Grants permission to start the channel with the specified channel name	Write	aws:TagKeys (p. 863)		
StopChannel	Grants permission to stop the channel with the specified channel name	Write	channel* (p. 863)		
TagResource	Grants permission to add tags to the specified playback configuration resource	Tagging	channel (p. 863)		
			liveSource (p. 863)		
			playbackConfiguration (p. 863)		
			sourceLocation (p. 863)		
			vodSource (p. 863)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 863) aws:TagKeys (p. 863)	
UntagResource	Grants permission to remove tags from the specified playback configuration resource	Tagging	channel (p. 863) liveSource (p. 863) playbackConfiguration (p. 863)		
			sourceLocation (p. 863)		
			vodSource (p. 863)		
			aws:RequestTag/ \${TagKey} (p. 863) aws:TagKeys (p. 863)		
UpdateChannel	Grants permission to update the channel with the specified channel name	Write	channel* (p. 863)		
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* (p. 863)		
			sourceLocation* (p. 863)		
UpdateSourceLocation	Grants permission to update the source location with the specified source location name	Write	sourceLocation* (p. 863)		
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	sourceLocation* (p. 863)		
			vodSource* (p. 863)		

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 \(p. 858\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 863)
prefetchSchedule	arn:\${Partition}:mediatailor:\${Region}: \${Account}:prefetchSchedule/\${ResourceId}	
channel	arn:\${Partition}:mediatailor:\${Region}: \${Account}:channel/\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 863)
program	arn:\${Partition}:mediatailor:\${Region}: \${Account}:program/\${ResourceId}	
sourceLocation	arn:\${Partition}:mediatailor:\${Region}: \${Account}:sourceLocation/\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 863)
vodSource	arn:\${Partition}:mediatailor:\${Region}: \${Account}:vodSource/\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 863)
liveSource	arn:\${Partition}:mediatailor:\${Region}: \${Account}:liveSource/\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 863)

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 [Available global condition 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 Elemental Support Cases

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 Elemental Support Cases \(p. 864\)](#)
- [Resource types defined by Elemental Support Cases \(p. 864\)](#)
- [Condition keys for Elemental Support Cases \(p. 865\)](#)

Actions defined by 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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CheckCasePermissions [permission only]	Verify whether the caller has the permissions to perform support case operations	Write			
CreateCase [permission only]	Grant the permission to create a support case	Write			
GetCase [permission only]	Grant the permission to describe a support case in your account	Read			
GetCases [permission only]	Grant the permission to list the support cases in your account	Read			
UpdateCase [permission only]	Grant the permission to update a support case	Write			

Resource types defined by Elemental Support Cases

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

Condition keys for Elemental Support Cases

Elemental Support Cases 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 [Available keys for conditions](#).

Actions, resources, and condition keys for Elemental Support Content

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 Elemental Support Content \(p. 865\)](#)
- [Resource types defined by Elemental Support Content \(p. 866\)](#)
- [Condition keys for Elemental Support Content \(p. 866\)](#)

Actions defined by 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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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]	Grant the permission to search support content	Read			

Resource types defined by Elemental Support Content

Elemental Support Content does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Elemental Support Content, specify “`Resource`”: “`*`” in your policy.

Condition keys for 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 [Available keys for conditions](#).

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 \(EMR Containers\) \(p. 866\)](#)
- [Resource types defined by Amazon EMR on EKS \(EMR Containers\) \(p. 868\)](#)
- [Condition keys for Amazon EMR on EKS \(EMR Containers\) \(p. 868\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources (“`*`”) in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 868)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateManagedEndpoint	Grants permission to create a managed endpoint	Write	virtualCluster* (p. 868)		
			aws:RequestTag/ {\$TagKey} (p. 869)		
	Grants permission to create a virtual cluster	Write	aws:RequestTag/ {\$TagKey} (p. 869)		aws:TagKeys (p. 869)
DeleteManagedEndpoint	Grants permission to delete a managed endpoint	Write	managedEndpoint* (p. 868)		
DeleteVirtualCluster	Grants permission to delete a virtual cluster	Write	virtualCluster* (p. 868)		
DescribeJobRun	Grants permission to describe a job run	Read	jobRun* (p. 868)		
DescribeManagedEndpoint	Grants permission to describe a managed endpoint	Read	managedEndpoint* (p. 868)		
DescribeVirtualCluster	Grants permission to describe a virtual cluster	Read	virtualCluster* (p. 868)		
ListJobRuns	Grants permission to list job runs associated with a virtual cluster	List	virtualCluster* (p. 868)		
ListManagedEndpoints	Grants permission to list managed endpoints associated with a virtual cluster	List	virtualCluster* (p. 868)		
ListTagsForResource	Grants permission to list tags for the specified resource	List	jobRun (p. 868) managedEndpoint (p. 868) virtualCluster (p. 868)		
ListVirtualClusters	Grants permission to list virtual clusters	List			
StartJobRun	Grants permission to start a job run	Write	virtualCluster* (p. 868)		
			aws:RequestTag/ {\$TagKey} (p. 869)		
			aws:TagKeys (p. 869)		
			emr- containers:ExecutionRoleArn (p. 869)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to tag the specified resource	Tagging	jobRun (p. 868) managedEndpoint (p. 868) virtualCluster (p. 868)		
				aws:RequestTag/ {\$TagKey} (p. 869)	
				aws:TagKeys (p. 869)	
UntagResource	Grants permission to untag the specified resource	Tagging	jobRun (p. 868) managedEndpoint (p. 868) virtualCluster (p. 868)		
				aws:TagKeys (p. 869)	

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 \(p. 866\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 869)
jobRun	arn:\${Partition}:emr-containers:\${Region}:\${Account}:/virtualclusters/\${virtualClusterId}/jobruns/\${jobRunId}	aws:ResourceTag/ {\$TagKey} (p. 869)
managedEndpoint	arn:\${Partition}:emr-containers:\${Region}:\${Account}:/virtualclusters/\${virtualClusterId}/endpoints/\${endpointId}	aws:ResourceTag/ {\$TagKey} (p. 869)

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters actions based on the presence of tag key-value pairs in the request	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters actions based on tag key-value pairs attached to the resource	String
<code>aws:TagKeys</code>	Filters actions based on the presence of tag keys in the request	String
<code>emr-containers:ExecutionProviderArn</code>	Filters actions based on whether the execution role arn is provided with the action	String

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 \(p. 869\)](#)
- [Resource types defined by Amazon EMR Serverless \(p. 871\)](#)
- [Condition keys for Amazon EMR Serverless \(p. 871\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 871)		
CreateApplication	Grants permission to create an Application	Write		aws:RequestTag/\${TagKey} (p. 871) aws:TagKeys (p. 871)	
DeleteApplication	Grants permission to delete an application	Write	application* (p. 871)		
GetApplication	Grants permission to get application	Read	application* (p. 871)		
GetJobRun	Grants permission to get a job run	Read	jobRun* (p. 871)		
ListApplications	Grants permission to list applications	List			
ListJobRuns	Grants permission to list job runs associated with an application	List	application* (p. 871)		
ListTagsForResource	Grants permission to list tags for the specified resource	Read	application (p. 871) jobRun (p. 871)		
StartApplication	Grants permission to Start an application	Write	application* (p. 871)		
StartJobRun	Grants permission to start a job run	Write	application* (p. 871) aws:RequestTag/\${TagKey} (p. 871) aws:TagKeys (p. 871)	iam:PassRole	
StopApplication	Grants permission to Stop an application	Write	application* (p. 871)		
TagResource	Grants permission to tag the specified resource	Tagging	application (p. 871) jobRun (p. 871) aws:RequestTag/\${TagKey} (p. 871) aws:TagKeys (p. 871)		
UntagResource	Grants permission to untag the specified resource	Tagging	application (p. 871) jobRun (p. 871) aws:TagKeys (p. 871)		
UpdateApplication	Grants permission to Update an application	Write	application* (p. 871)		

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 \(p. 869\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
application	<code>arn:\${Partition}:emr-serverless:\${Region}: \${Account}:/applications/\${ApplicationId}</code>	aws:ResourceTag/\${TagKey} (p. 871)
jobRun	<code>arn:\${Partition}:emr-serverless:\${Region}: \${Account}:/applications/\${ApplicationId}/ jobruns/\${JobRunId}</code>	aws:ResourceTag/\${TagKey} (p. 871)

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 [Available global condition 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 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 \(p. 872\)](#)
- [Resource types defined by Amazon EventBridge \(p. 877\)](#)
- [Condition keys for Amazon EventBridge \(p. 877\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 877)		
CancelReplay	Grants permission to cancel a replay	Write	replay* (p. 877)		
CreateApiDestination	Grants permission to create a new api destination	Write	api-destination* (p. 877)		
			connection* (p. 877)		
CreateArchive	Grants permission to create a new archive	Write	archive* (p. 877)		
CreateConnection	Grants permission to create a new connection	Write	connection* (p. 877)		
CreateEndpoint	Grants permission to create an endpoint	Write	endpoint* (p. 877)		
				events:EventBusArn (p. 878)	
CreateEventBus	Grants permission to create event buses	Write	event-bus* (p. 877)		
				aws:RequestTag/\$[TagKey] (p. 877)	
				aws:TagKeys (p. 877)	
CreatePartnerEventSource	Grants permission to create partner event sources	Write	event-source* (p. 877)		
DeactivateEventSource	Grants permission to deactivate event sources	Write	event-source* (p. 877)		
DeauthorizeConnection	Grants permission to deauthorize a connection,	Write	connection* (p. 877)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	deleting its stored authorization secrets				
DeleteApiDestination	Grants permission to delete an api destination	Write	api-destination* (p. 877)		
DeleteArchive	Grants permission to delete an archive	Write	archive* (p. 877)		
DeleteConnection	Grants permission to delete a connection	Write	connection* (p. 877)		
DeleteEndpoint	Grants permission to delete an endpoint	Write	endpoint* (p. 877)		
DeleteEventBus	Grants permission to delete event buses	Write	event-bus* (p. 877)		
DeletePartnerEventSource	Grants permission to delete partner event sources	Write	event-source* (p. 877)		
DeleteRule	Grants permission to delete rules	Write	rule* (p. 877)		
				events:creatorAccount (p. 878)	
				events:ManagedBy (p. 878)	
DescribeApiDestination	Grants permission to retrieve details about an api destination	Read	api-destination* (p. 877)		
			connection* (p. 877)		
DescribeArchive	Grants permission to retrieve details about an archive	Read	archive* (p. 877)		
DescribeConnection	Grants permission to retrieve details about a connection	Read	connection* (p. 877)		
DescribeEndpoint	Grants permission to retrieve details about an endpoint	Read	endpoint* (p. 877)		
DescribeEventBus	Grants permission to retrieve details about event buses	Read	event-bus (p. 877)		
DescribeEventSource	Grants permission to retrieve details about event sources	Read	event-source* (p. 877)		
DescribePartnerEventSource	Grants permission to retrieve details about partner event sources	Read	event-source* (p. 877)		
DescribeReplay	Grants permission to retrieve the details of a replay	Read	replay* (p. 877)		
DescribeRule	Grants permission to retrieve details about rules	Read	rule* (p. 877)		
				events:creatorAccount (p. 878)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableRule	Grants permission to disable rules	Write	rule* (p. 877)		
			events:creatorAccount (p. 878)	events:ManagedBy (p. 878)	
EnableRule	Grants permission to enable rules	Write	rule* (p. 877)		
			events:creatorAccount (p. 878)	events:ManagedBy (p. 878)	
InvokeApiDestination [permission only]	Grants permission to invoke an api destination	Write	api-destination* (p. 877)		
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 retrieve a list of event sources shared with this account	List			
ListPartnerEvents	Grants permission to retrieve a list of AWS account IDs associated with an event source	List	event-source* (p. 877)		
ListPartnerEventSources	Grants permission to retrieve a list of partner event sources	List			
ListReplays	Grants permission to retrieve a list of replays	List			
ListRuleNamesByTarget	Grants permission to retrieve a list of the names of the rules associated with a target	List			
ListRules	Grants permission to retrieve a list of the Amazon EventBridge rules in the account	List			

Service Authorization Reference
Service Authorization Reference
Amazon EventBridge

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to retrieve a list of tags associated with an Amazon EventBridge resource	List	event-bus (p. 877)		
	rule (p. 877)				
				events:creatorAccount (p. 878)	
ListTargetsByRule	Grants permission to retrieve a list of targets defined for a rule	List	rule* (p. 877)		
				events:creatorAccount (p. 878)	
PutEvents	Grants permission to send custom events to Amazon EventBridge	Write	event-bus* (p. 877)		
				events:detail-type (p. 878)	
				events:source (p. 878)	
				events:eventBusInvocation (p. 878)	
PutPartnerEvents	Grants permission to send custom events to Amazon EventBridge	Write			
PutPermission	Grants permission to use the PutPermission action to grants permission to another AWS account to put events to your default event bus	Permissions management			
PutRule	Grants permission to create or updates rules	Write	rule* (p. 877)		
				events:detail.userIdentity.principalId (p. 877)	
				events:detail-type (p. 878)	
				events:source (p. 878)	
				events:detail.service (p. 878)	
				events:detail.eventTypeCode (p. 878)	
				aws:RequestTag/\${TagKey} (p. 877)	
				aws:TagKeys (p. 877)	
				events:creatorAccount (p. 878)	
PutTargets	Grants permission to add targets to a rule	Write	rule* (p. 877)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					events:TargetArn (p. 878) events:creatorAccount (p. 878) events:ManagedBy (p. 878)
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* (p. 877)		
					events:creatorAccount (p. 878) events:ManagedBy (p. 878)
StartReplay	Grants permission to start a replay of an archive	Write	archive* (p. 877)		
TagResource	Grants permission to add a tag to an Amazon EventBridge resource	Tagging	event-bus (p. 877)		
			rule (p. 877)		
					aws:TagKeys (p. 877) aws:RequestTag/\${TagKey} (p. 877) events:creatorAccount (p. 878)
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 (p. 877)		
			rule (p. 877)		
					aws:TagKeys (p. 877) events:creatorAccount (p. 878)
UpdateApiDestination	Grants permission to update an api destination	Write	api-destination* (p. 877)		
UpdateArchive	Grants permission to update an archive	Write	archive* (p. 877)		
UpdateConnection	Grants permission to update a connection	Write	connection* (p. 877)		
UpdateEndpoint	Grants permission to update an endpoint	Write	endpoint* (p. 877)		
					events:EventBusArn (p. 878)

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 \(p. 872\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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}	
event-bus	arn:\${Partition}:events:\${Region}: \${Account}:event-bus/\${EventBusName}	aws:ResourceTag/ \${TagKey} (p. 877)
rule	arn:\${Partition}:events: \${Region}: \${Account}:rule/ [\${EventBusName}/]\${RuleName}	aws:ResourceTag/ \${TagKey} (p. 877)
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}	

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 [Available global condition 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

Condition keys	Description	Type
events:EventBusArn	Filters access by the ARN of the event buses that can be associated with an endpoint to CreateEndpoint and UpdateEndpoint actions	ArrayOfARN
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	ArrayOfARN
events:creatorAccount	Filters access by the account the rule was created in to rule actions	String
events:detail-type	Filters access by the literal string of the detail-type of the event to PutEvents and PutRule actions	String
events:detail.eventTypeCode	Filters access by the literal string for the detail.eventTypeCode field of the event to PutRule actions	String
events:detail.service	Filters access by the literal string for the detail.service field of the event to PutRule actions	String
events:detail.userIdentity.principalId	Filters access by the literal string for the detail.userIdentity.principalId field of the event to PutRule actions	String
events:eventBusInvocationAccount	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 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 \(p. 879\)](#)
- [Resource types defined by Amazon EventBridge Schemas \(p. 882\)](#)
- [Condition keys for Amazon EventBridge Schemas \(p. 882\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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	discoverer* (p. 882)		
			aws:RequestTag/\${TagKey} (p. 882)		
			aws:TagKeys (p. 882)		
CreateRegistry	Grants permission to create a new schema registry in your account	Write	registry* (p. 882)		
			aws:RequestTag/\${TagKey} (p. 882)		
			aws:TagKeys (p. 882)		
CreateSchema	Grants permission to create a new schema in your account	Write	schema* (p. 882)		
			aws:RequestTag/\${TagKey} (p. 882)		
			aws:TagKeys (p. 882)		
DeleteDiscoverer	Grants permission to delete discoverer in your account	Write	discoverer* (p. 882)		
DeleteRegistry	Grants permission to delete an existing registry in your account	Write	registry* (p. 882)		
DeleteResourcePolicy	Grants permission to delete the resource-based policy attached to a given registry	Write	registry* (p. 882)		
DeleteSchema	Grants permission to delete an existing schema in your account	Write	schema* (p. 882)		
DeleteSchemaVersion	Grants permission to delete a specific version of schema in your account	Write	schema* (p. 882)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeCodeBinding	Grants permission to retrieve metadata for generated code for specific schema in your account	Read	schema* (p. 882)		
DescribeDiscoverer	Grants permission to retrieve discoverer metadata in your account	Read	discoverer* (p. 882)		
DescribeRegistry	Grants permission to describe an existing registry metadata in your account	Read	registry* (p. 882)		
DescribeSchema	Grants permission to retrieve an existing schema in your account	Read	schema* (p. 882)		
ExportSchema	Grants permission to export the AWS registry or discovered schemas in OpenAPI 3 format to JSONSchema format	Read	registry* (p. 882)		
GetCodeBinding	Grants permission to retrieve metadata for generated code for specific schema in your account		schema* (p. 882)		
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* (p. 882)		
ListDiscoverers	Grants permission to list all discoverers in your account	List	discoverer* (p. 882)		
ListRegistries	Grants permission to list all registries in your account	List	registry* (p. 882)		
ListSchemaVersions	Grants permission to list all versions of a schema	List	schema* (p. 882)		
ListSchemas	Grants permission to list all schemas	List	schema* (p. 882)		
ListTagsForResource	Grants permission to lists tags for a resource	Read	discoverer (p. 882)		
			registry (p. 882)		
			schema (p. 882)		
PutCodeBinding	Grants permission to generate code for specific schema in your account	Write	schema* (p. 882)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutResourcePolicy	Grants permission to attach a resource-based policy to a given registry	Write	registry* (p. 882)		
SearchSchemas	Grants permission to search schemas based on specified keywords in your account	List	schema* (p. 882)		
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* (p. 882)		
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* (p. 882)		
TagResource	Grants permission to tag a resource	Tagging	discoverer (p. 882)		
			registry (p. 882)		
			schema (p. 882)		
				aws:TagKeys (p. 882)	
				aws:RequestTag/ \${TagKey} (p. 882)	
UntagResource	Grants permission to remove a tag from a resource	Tagging	discoverer (p. 882)		
			registry (p. 882)		
			schema (p. 882)		
				aws:TagKeys (p. 882)	
UpdateDiscoverer	Grants permission to update an existing discoverer in your account	Write	discoverer* (p. 882)		
UpdateRegistry	Grants permission to update an existing registry metadata in your account	Write	registry* (p. 882)		
UpdateSchema	Grants permission to update an existing schema in your account	Write	schema* (p. 882)		

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 \(p. 879\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
discoverer	<code>arn:\${Partition}:schemas:\${Region}: \${Account}:discoverer/\${DiscovererId}</code>	aws:ResourceTag/\${TagKey} (p. 882)
registry	<code>arn:\${Partition}:schemas:\${Region}: \${Account}:registry/\${RegistryName}</code>	aws:ResourceTag/\${TagKey} (p. 882)
schema	<code>arn:\${Partition}:schemas:\${Region}: \${Account}:schema/\${RegistryName}/ \${SchemaName}</code>	aws:ResourceTag/\${TagKey} (p. 882)

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 [Available global condition 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 Simulator

AWS Fault Injection Simulator (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 Simulator \(p. 883\)](#)
- [Resource types defined by AWS Fault Injection Simulator \(p. 885\)](#)
- [Condition keys for AWS Fault Injection Simulator \(p. 886\)](#)

Actions defined by AWS Fault Injection Simulator

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

The **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateExperiment <small>AWS FIS</small>	Grants permission to create an AWS FIS experiment template	Write	action* (p. 886)		
			experiment-template* (p. 886)		
			aws:RequestTag/ {\$TagKey} (p. 886)		
			aws:TagKeys (p. 886)		
DeleteExperiment <small>AWS FIS</small>	Grants permission to delete the AWS FIS experiment template	Write	experiment-template* (p. 886)		
GetAction	Grants permission to retrieve an AWS FIS action	Read	action* (p. 886)		
			aws:ResourceTag/ {\$TagKey} (p. 886)		
GetExperiment	Grants permission to retrieve an AWS FIS experiment	Read	experiment* (p. 886)		
			aws:ResourceTag/ {\$TagKey} (p. 886)		
GetExperimentTemplate <small>AWS FIS</small>	Grants permission to retrieve an AWS FIS Experiment Template	Read	experiment-template* (p. 886)		
			aws:ResourceTag/ {\$TagKey} (p. 886)		
GetTargetResourceInfo	Grants permission to get information about the specified resource type	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
InjectApiInternalError	Grants permission to inject API internal error on the provided AWS service from an FIS Experiment	Write	experiment* (p. 886)		
			fis:Service (p. 886)		
			fis:Operations (p. 886)		
			fis:Percentage (p. 886)		
			fis:Targets (p. 886)		
InjectApiThrottleError	Grants permission to inject API throttle error on the provided AWS service from an FIS Experiment	Write	experiment* (p. 886)		
			fis:Service (p. 886)		
			fis:Operations (p. 886)		
			fis:Percentage (p. 886)		
			fis:Targets (p. 886)		
ListActions	Grants permission to list all available AWS FIS actions	List			
ListExperimentTemplates	Grants permission to list all available AWS FIS experiment templates	List			
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 (p. 886)		
			experiment (p. 886)		
			experiment-template (p. 886)		
ListTargetResourceTypes	Grants permission to list the resource types	List			
StartExperiment	Grants permission to run an AWS FIS experiment	Write	experiment* (p. 886)	iam:CreateServiceLinkedRole	
			experiment-template* (p. 886)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 886) aws:TagKeys (p. 886)	
StopExperiment	Grants permission to stop an AWS FIS experiment	Write	experiment* (p. 886)		
TagResource	Grants permission to tag AWS FIS resources	Tagging	action (p. 886)		
			experiment (p. 886)		
			experiment-template (p. 886)		
				aws:TagKeys (p. 886) aws:RequestTag/ \${TagKey} (p. 886)	
UntagResource	Grants permission to untag AWS FIS resources	Tagging	action (p. 886)		
			experiment (p. 886)		
			experiment-template (p. 886)		
				aws:TagKeys (p. 886) aws:RequestTag/ \${TagKey} (p. 886)	
UpdateExperiment	Grants permission to update the specified AWS FIS experiment template	Write	experiment-template* (p. 886)		
			action (p. 886)		
				aws:RequestTag/ \${TagKey} (p. 886) aws:TagKeys (p. 886)	

Resource types defined by AWS Fault Injection Simulator

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the [Actions table \(p. 883\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 886)
experiment	arn:\${Partition}:fis:\${Region}: \${Account}:experiment/\${Id}	aws:ResourceTag/\${TagKey} (p. 886)
experiment-template	arn:\${Partition}:fis:\${Region}: \${Account}:experiment-template/\${Id}	aws:ResourceTag/\${TagKey} (p. 886)

Condition keys for AWS Fault Injection Simulator

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

To view the global condition keys that are available to all services, see [Available global condition 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
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 \(p. 887\)](#)
- [Resource types defined by Amazon FinSpace \(p. 888\)](#)
- [Condition keys for Amazon FinSpace \(p. 889\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 a FinSpace environment	Write	environment*	(p. 888)	
				aws:TagKeys	(p. 889)
				aws:RequestTag/\${TagKey}	(p. 889)
CreateUser [permission only]	Grants permission to create a FinSpace user	Write	environment*	(p. 888)	
			user*	(p. 888)	
				aws:TagKeys	(p. 889)
				aws:RequestTag/\${TagKey}	(p. 889)
DeleteEnvironment	Grants permission to delete a FinSpace environment	Write	environment*	(p. 888)	
GetEnvironment	Grants permission to describe a FinSpace environment	Read	environment*	(p. 888)	
GetLoadSampleData [permission only]	Grants permission to request status of the loading of sample data bundle	Read	environment*	(p. 888)	
 GetUser [permission only]	Grants permission to describe a FinSpace user	Read	environment*	(p. 888)	
				user*	(p. 888)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListEnvironments	Grants permission to list FinSpace environments in the AWS account	List	environment* (p. 888)		
ListTagsForResource	Grants permission to return a list of tags for a resource	Read	environment* (p. 888)		
ListUsers [permission only]	Grants permission to list FinSpace users in an environment	List	environment* (p. 888)		
			user* (p. 888)		
LoadSampleData [permission only]	Grants permission to load Sample data bundle into your FinSpace environment	Write	environment* (p. 888)		
ResetUserPassword [permission only]	Grants permission to reset the password for a FinSpace user	Write	environment* (p. 888)		
			user* (p. 888)		
TagResource	Grants permission to tag a resource	Tagging	environment* (p. 888)		
UntagResource	Grants permission to untag a resource	Tagging	environment* (p. 888)		
UpdateEnvironment	Grants permission to update a FinSpace environment	Write	environment* (p. 888)		
UpdateUser [permission only]	Grants permission to update a FinSpace user	Write	environment* (p. 888)		
			user* (p. 888)		

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 \(p. 887\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
environment	<code>arn:\${Partition}:finspace:\${Region}: \${Account}:environment/\${EnvironmentId}</code>	aws:ResourceTag/\${TagKey} (p. 889)
user	<code>arn:\${Partition}:finspace:\${Region}: \${Account}:user/\${UserId}</code>	aws:ResourceTag/\${TagKey} (p. 889)

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 [Available global condition keys](#).

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

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 \(p. 889\)](#)
- [Resource types defined by AWS Firewall Manager \(p. 893\)](#)
- [Condition keys for AWS Firewall Manager \(p. 893\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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			
AssociateThirdPartyFirewallManager	Grants permission to set the Firewall Manager administrator as a tenant administrator of a third-party firewall service	Write			
DeleteAppsList	Grants permission to permanently deletes an AWS Firewall Manager applications list	Write	applications-list* (p. 893)		
DeleteNotificationChannel	Grants permission to delete 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* (p. 893)		
				aws:ResourceTag/\${TagKey} (p. 894)	
DeleteProtocolsList	Grants permission to permanently deletes an AWS Firewall Manager protocols list	Write	protocols-list* (p. 893)		
DisassociateAdminAccount	Grants permission to disassociate the account that has been set as the AWS Firewall Manager administrator account and disables the service in all organization accounts	Write			
DisassociateThirdPartyFirewallManager	Grants permission to disassociate Firewall Manager administrator from a third-party firewall tenant	Write			
GetAdminAccount	Grants permission to retrieve the AWS Organizations master account that is associated with AWS Firewall Manager	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	as the AWS Firewall Manager administrator				
GetAppsList	Grants permission to return information about the specified AWS Firewall Manager applications list	Read	applications-list* (p. 893)		
GetComplianceDetails	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* (p. 893)		
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* (p. 893)		
GetProtectionStatus	Grants permission to retrieve policy-level attack summary information in the event of a potential DDoS attack	Read	policy* (p. 893)		
GetProtocolsList	Grants permission to return information about the specified AWS Firewall Manager protocols list	Read	protocols-list* (p. 893)		
GetThirdPartyFirewallOnboardingStatus	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* (p. 893)		
ListAppsLists	Grants permission to return an array of AppsListDataSummary objects	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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* (p. 893)		
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			
ListProtocolsLists	Grants permission to return an array of ProtocolsListDataSummary objects	List			
ListTagsForResource	Grants permission to list Tags for a given resource	Read	policy* (p. 893)		
ListThirdPartyFirewallPolicies	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			
PutAppsList	Grants permission to create an AWS Firewall Manager applications list	Write	applications-list* (p. 893)		
				aws:RequestTag/\${TagKey} (p. 893)	aws:TagKeys (p. 894)
PutNotificationClient	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* (p. 893)		
				aws:RequestTag/\${TagKey} (p. 893)	aws:TagKeys (p. 894)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutProtocolsList	Grants permission to creates an AWS Firewall Manager protocols list	Write	protocols-list* (p. 893)		
				aws:RequestTag/\${TagKey} (p. 893) aws:TagKeys (p. 894)	
TagResource	Grants permission to add a Tag to a given resource	Tagging	policy* (p. 893)		
				aws:RequestTag/\${TagKey} (p. 893) aws:TagKeys (p. 894)	
UntagResource	Grants permission to remove a Tag from a given resource	Tagging	policy* (p. 893)		
				aws:TagKeys (p. 894)	

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 \(p. 889\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 894)
applications-list	arn:\${Partition}:fms:\${Region}: \${Account}:applications-list/\${Id}	aws:ResourceTag/\${TagKey} (p. 894)
protocols-list	arn:\${Partition}:fms:\${Region}: \${Account}:protocols-list/\${Id}	aws:ResourceTag/\${TagKey} (p. 894)

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 [Available global condition 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 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 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 \(p. 894\)](#)
- [Resource types defined by Amazon Forecast \(p. 899\)](#)
- [Condition keys for Amazon Forecast \(p. 900\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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} (p. 900) aws:TagKeys (p. 900)	
CreateDataset	Grants permission to create a dataset	Write	dataset* (p. 899)		

Service Authorization Reference
Service Authorization Reference
Amazon Forecast

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 900) aws:TagKeys (p. 900)	
CreateDatasetGroup	Grants permission to create a dataset group	Write	datasetGroup* (p. 899)		
				aws:RequestTag/ \${TagKey} (p. 900) aws:TagKeys (p. 900)	
CreateDatasetImportJob	Grants permission to create a dataset import job	Write	datasetImportJob* (p. 899)		
				aws:RequestTag/ \${TagKey} (p. 900) aws:TagKeys (p. 900)	
CreateExplainabilityExport	Grants permission to create an explainability export	Write	forecast* (p. 900)		
				aws:RequestTag/ \${TagKey} (p. 900) aws:TagKeys (p. 900)	
CreateExplainabilityExport	Grants permission to create an explainability export using an explainability resource	Write	explainability* (p. 900)		
				aws:RequestTag/ \${TagKey} (p. 900) aws:TagKeys (p. 900)	
CreateForecast	Grants permission to create a forecast	Write	predictor* (p. 899)		
				aws:RequestTag/ \${TagKey} (p. 900) aws:TagKeys (p. 900)	
CreateForecastExport	Grants permission to create a forecast export job using a forecast resource	Write	forecast* (p. 900)		
				aws:RequestTag/ \${TagKey} (p. 900) aws:TagKeys (p. 900)	
CreatePredictor	Grants permission to create a predictor	Write	datasetGroup* (p. 899)		
				aws:RequestTag/ \${TagKey} (p. 900) aws:TagKeys (p. 900)	
CreatePredictorBatch	Grants permission to create a predictor batch export job using a predictor	Write	predictor* (p. 899)		

Service Authorization Reference
Service Authorization Reference
Amazon Forecast

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 900) aws:TagKeys (p. 900)	
DeleteDataset	Grants permission to delete a dataset	Write	dataset* (p. 899)		
DeleteDatasetGroup	Grants permission to delete a dataset group	Write	datasetGroup* (p. 899)		
DeleteDatasetImportJob	Grants permission to delete a dataset import job	Write	datasetImportJob* (p. 899)		
DeleteExplainability	Grants permission to delete an explainability	Write	explainability* (p. 900)		
DeleteExplainabilityExport	Grants permission to delete an explainability export	Write	explainabilityExport* (p. 900)		
DeleteForecast	Grants permission to delete a forecast	Write	forecast* (p. 900)		
DeleteForecastExportJob	Grants permission to delete a forecast export job	Write	forecastExport* (p. 900)		
DeletePredictor	Grants permission to delete a predictor	Write	predictor* (p. 899)		
DeletePredictorBacktestExportJob	Grants permission to delete a predictor backtest export job	Write	predictorBacktestExportJob* (p. 899)		
DeleteResourceTree	Grants permission to delete a resource and its child resources	Write	dataset* (p. 899) datasetGroup* (p. 899) datasetImportJob* (p. 899) explainability* (p. 900) explainabilityExport* (p. 900) forecast* (p. 900) forecastExport* (p. 900) predictor* (p. 899) predictorBacktestExportJob* (p. 899)		
DescribeAutoPredictor	Grants permission to describe an auto predictor	Read	predictor* (p. 899)		
DescribeDataset	Grants permission to describe a dataset	Read	dataset* (p. 899)		

Service Authorization Reference
Service Authorization Reference
Amazon Forecast

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDatasetGroup	Grants permission to describe a dataset group	Read	datasetGroup* (p. 899)		
DescribeDatasetImportJob	Grants permission to describe a dataset import job	Read	datasetImportJob* (p. 899)		
DescribeExplainability	Grants permission to describe an explainability	Read	explainability* (p. 900)		
DescribeExplainabilityExport	Grants permission to describe an explainability export	Read	explainabilityExport* (p. 900)		
DescribeForecast	Grants permission to describe a forecast	Read	forecast* (p. 900)		
DescribeForecastExportJob	Grants permission to describe a forecast export job	Read	forecastExport* (p. 900)		
DescribePredictor	Grants permission to describe a predictor	Read	predictor* (p. 899)		
DescribePredictorBacktestExportJob	Grants permission to describe a predictor backtest export job	Read	predictorBacktestExportJob* (p. 899)		
GetAccuracyMetrics	Grants permission to get the Accuracy Metrics for a predictor	Read	predictor* (p. 899)		
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			
ListForecastExports	Grants permission to list all the forecast export jobs	Read			
ListForecasts	Grants permission to list all the forecasts	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 (p. 899) datasetGroup (p. 899)		

Service Authorization Reference
 Service Authorization Reference
 Amazon Forecast

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			datasetImportJob (p. 899) explainability (p. 900) explainabilityExport (p. 900) forecast (p. 900) forecastExport (p. 900) predictor (p. 899) predictorBacktestExportJob (p. 899)		
QueryForecast	Grants permission to retrieve a forecast for a single item	Read	forecast* (p. 900)		
StopResource	Grants permission to stop Amazon Forecast resource jobs	Write	datasetImportJob* (p. 899) explainability* (p. 900) explainabilityExport* (p. 900) forecast* (p. 900) forecastExport* (p. 900) predictor* (p. 899) predictorBacktestExportJob* (p. 899)		aws:RequestTag/\${TagKey} (p. 900) aws:TagKeys (p. 900)
TagResource	Grants permission to associate the specified tags to a resource	Tagging	dataset (p. 899) datasetGroup (p. 899) datasetImportJob (p. 899) explainability (p. 900) explainabilityExport (p. 900) forecast (p. 900) forecastExport (p. 900) predictor (p. 899) predictorBacktestExportJob (p. 899)		aws:RequestTag/\${TagKey} (p. 900) aws:TagKeys (p. 900)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagResource	Grants permission to delete the specified tags for a resource	Tagging	dataset (p. 899) datasetGroup (p. 899) datasetImportJob (p. 899) explainability (p. 900) explainabilityExport (p. 900) forecast (p. 900) forecastExport (p. 900) predictor (p. 899) predictorBacktestExportJob (p. 899)		
				aws:TagKeys (p. 900)	
UpdateDatasetGroup	Grants permission to update a dataset group	Write	dataset* (p. 899) datasetGroup* (p. 899)		

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 \(p. 894\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 900)
datasetGroup	arn:\${Partition}:forecast:\${Region}: \${Account}:dataset-group/\${ResourceId}	aws:ResourceTag/ \${TagKey} (p. 900)
datasetImportJob	arn:\${Partition}:forecast:\${Region}: \${Account}:dataset-import-job/\${ResourceId}	aws:ResourceTag/ \${TagKey} (p. 900)
algorithm	arn:\${Partition}:forecast:::algorithm/ \${ResourceId}	
predictor	arn:\${Partition}:forecast:\${Region}: \${Account}:predictor/\${ResourceId}	aws:ResourceTag/ \${TagKey} (p. 900)
predictorBacktestExportJob	arn:\${Partition}:forecast:\${Region}: \${Account}:predictor-backtest-export-job/ \${ResourceId}	aws:ResourceTag/ \${TagKey} (p. 900)

Resource types	ARN	Condition keys
forecast	arn:\${Partition}:forecast:\${Region}: \${Account}:forecast/\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 900)
forecastExport	arn:\${Partition}:forecast:\${Region}: \${Account}:forecast-export-job/\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 900)
explainability	arn:\${Partition}:forecast:\${Region}: \${Account}:explainability/\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 900)
explainabilityExport	arn:\${Partition}:forecast:\${Region}: \${Account}:explainability-export/\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 900)

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 [Available global condition 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 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 \(p. 901\)](#)
- [Resource types defined by Amazon Fraud Detector \(p. 913\)](#)
- [Condition keys for Amazon Fraud Detector \(p. 914\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchCreateVariables	Grants permission to create a batch of variables	Write		aws:RequestTag/\${TagKey} (p. 914) aws:TagKeys (p. 914)	
BatchGetVariable	Grants permission to get a batch of variables	List	variable*	(p. 914)	
CancelBatchImport	Grants permission to cancel the specified batch import job	Write	batch-import*	(p. 914)	
CancelBatchPrediction	Grants permission to cancel the specified batch prediction job	Write	batch-prediction*	(p. 913)	
CreateBatchImport	Grants permission to create a batch import job	Write	batch-import*	(p. 914)	
			event-type*	(p. 914)	
				aws:RequestTag/\${TagKey} (p. 914) aws:TagKeys (p. 914)	
CreateBatchPrediction	Grants permission to create a batch prediction job	Write	batch-prediction*	(p. 913)	
			detector*	(p. 913)	
			detector-version*	(p. 913)	
			event-type*	(p. 914)	
				aws:RequestTag/\${TagKey} (p. 914)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys (p. 914)	
CreateDetectorVersion	Grants permission to create a detector version. The detector version starts in a DRAFT status	Write	detector* (p. 913)		
			external-model (p. 914)		
			model-version (p. 914)		
				aws:RequestTag/ \${TagKey} (p. 914)	aws:TagKeys (p. 914)
CreateModel	Grants permission to create a model using the specified model type	Write	event-type* (p. 914)		
			model* (p. 914)		
				aws:RequestTag/ \${TagKey} (p. 914)	aws:TagKeys (p. 914)
CreateModelVersion	Grants permission to create a version of the model using the specified model type and model id	Write	model* (p. 914)		
				aws:RequestTag/ \${TagKey} (p. 914)	
				aws:TagKeys (p. 914)	
CreateRule	Grants permission to create a rule for use with the specified detector	Write	detector* (p. 913)		
				aws:RequestTag/ \${TagKey} (p. 914)	
				aws:TagKeys (p. 914)	
CreateVariable	Grants permission to create a variable	Write		aws:RequestTag/ \${TagKey} (p. 914)	
				aws:TagKeys (p. 914)	
DeleteBatchImportJob	Grants permission to delete a batch import job	Write	batch-import* (p. 914)		
DeleteBatchPredictionJob	Grants permission to delete a batch prediction job	Write	batch-prediction* (p. 913)		
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* (p. 913)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteDetectorVersion	Grants permission to delete the detector version. You cannot delete detector versions that are in ACTIVE status	Write	detector-version* (p. 913)		
DeleteEntityType	Grants permission to delete an entity type. You cannot delete an entity type that is included in an event type	Write	entity-type* (p. 913)		
DeleteEvent	Grants permission to deletes the specified event	Write	event-type* (p. 914)		
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* (p. 914)		
DeleteEventsByEventTypes	Grants permission to delete events for the specified event type	Write	event-type* (p. 914)		
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* (p. 914)		
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* (p. 914)		
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* (p. 914)		
DeleteModelErrors	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* (p. 914)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteOutcome	Grants permission to delete an outcome. You cannot delete an outcome that is used in a rule version	Write	outcome* (p. 914)		
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* (p. 914)		
DeleteVariable	Grants permission to delete a variable. You cannot delete variables that are included in an event type in Amazon Fraud Detector	Write	variable* (p. 914)		
DescribeDetector	Grants permission to get all versions for a specified detector	Read	detector* (p. 913)		
DescribeModelVersion	Grants permission to get all 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 (p. 914)		
GetBatchImportJobs	Grants permission to get all batch import jobs or a specific job if you specify a job ID	List	batch-import (p. 914)		
GetBatchPredictionJobs	Grants permission to get all 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 (p. 913)		
GetDeleteEventsByEventTypes	Grants permission to get specific event type DeleteEventsByEventType API execution status	Read	event-type* (p. 914)		
GetDetectorVersion	Grants permission to get a particular detector version	Read	detector-version* (p. 913)		

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 (p. 913)		
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 (p. 913)		
GetEvent	Grants permission to get the details of the specified event	Read	event-type* (p. 914)		
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* (p. 913)		
			detector-version* (p. 913)		
			event-type* (p. 914)		
GetEventPredictionDetails	Grants permission to get more details of a particular prediction	Read	detector* (p. 913)		
			detector-version* (p. 913)		
			event-type* (p. 914)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 (p. 914)		
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 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 GetExternalModelsResult as part of your request. A null pagination token fetches the records from the beginning	List	external-model (p. 914)		
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 pagination token from the GetGetLabelsResponse as part of your request. A null pagination token fetches the records from the beginning	List	label (p. 914)		
GetModelVersion	Grants permission to get the details of the specified model version	Read	model-version* (p. 914)		
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 (p. 914)		
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 (p. 914)		

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 (p. 914)		
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, provide a pagination token from GetVariablesResult as part of your request. Null pagination token fetches the records from the beginning	List	variable (p. 914)		
ListEventPredictions	Grants permission to get a list of past predictions	List	detector (p. 913)		
			detector-version (p. 913)		
			event-type (p. 914)		
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 (p. 914)		
			batch-prediction (p. 913)		
			detector (p. 913)		
			detector-version (p. 913)		
			entity-type (p. 913)		
			event-type (p. 914)		
			external-model (p. 914)		
			label (p. 914)		
			model (p. 914)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			model-version (p. 914)		
			outcome (p. 914)		
			rule (p. 914)		
			variable (p. 914)		
PutDetector	Grants permission to create or update a detector	Write	detector* (p. 913)		
			event-type* (p. 914)		
				aws:RequestTag/\${TagKey} (p. 914)	
				aws:TagKeys (p. 914)	
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* (p. 913)		
				aws:RequestTag/\${TagKey} (p. 914)	
				aws:TagKeys (p. 914)	
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* (p. 914)		
				aws:RequestTag/\${TagKey} (p. 914)	
				aws:TagKeys (p. 914)	

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* (p. 914)		
	external-model* (p. 914)				
	aws:RequestTag/\${TagKey} (p. 914)			aws:TagKeys (p. 914)	
PutKMSKey	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* (p. 914)		
			aws:RequestTag/\${TagKey} (p. 914)	aws:TagKeys (p. 914)	
PutOutcome	Grants permission to create or update an outcome	Write	outcome* (p. 914)		
			aws:RequestTag/\${TagKey} (p. 914)	aws:TagKeys (p. 914)	
SendEvent	Grants permission to send event	Write	event-type* (p. 914)		
			aws:RequestTag/\${TagKey} (p. 914)	aws:TagKeys (p. 914)	
TagResource	Grants permission to assign tags to a resource	Tagging	batch-import (p. 914)		
	batch-prediction (p. 913)				
	detector (p. 913)				
	detector-version (p. 913)				
	entity-type (p. 913)				

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			event-type (p. 914) external-model (p. 914) label (p. 914) model (p. 914) model-version (p. 914) outcome (p. 914) rule (p. 914) variable (p. 914) aws:TagKeys (p. 914) aws:RequestTag/\${TagKey} (p. 914)		
UntagResource	Grants permission to remove tags from a resource	Tagging	batch-import (p. 914) batch-prediction (p. 913) detector (p. 913) detector-version (p. 913) entity-type (p. 913) event-type (p. 914) external-model (p. 914) label (p. 914) model (p. 914) model-version (p. 914) outcome (p. 914) rule (p. 914) variable (p. 914)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys (p. 914) aws:RequestTag/\${TagKey} (p. 914)	
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* (p. 913)		
			external-model (p. 914)		
			model-version (p. 914)		
UpdateDetectorVersionDescription	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* (p. 913)		
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* (p. 913)		
UpdateEventLabel	Grants permission to update an existing event record's label value	Write	event-type* (p. 914)		
			aws:RequestTag/\${TagKey} (p. 914)		
			aws:TagKeys (p. 914)		
UpdateModel	Grants permission to update a model. You can update the description attribute using this action	Write	model* (p. 914)		

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* (p. 914)		
	aws:RequestTag/\${TagKey} (p. 914)		aws:TagKeys (p. 914)		
UpdateModelVersionStatus	Grants permission to update the status of a model version	Write	model-version* (p. 914)		
UpdateRuleMetadata	Grants permission to update a rule's metadata. The description attribute can be updated	Write	rule* (p. 914)		
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* (p. 914)		
aws:RequestTag/\${TagKey} (p. 914)	aws:TagKeys (p. 914)				
UpdateVariable	Grants permission to update a variable	Write	variable* (p. 914)		

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](#) (p. 901) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 914)
detector	arn:\${Partition}:frauddetector:\${Region}: \${Account}:detector/\${ResourcePath}	aws:ResourceTag/\${TagKey} (p. 914)
detector-version	arn:\${Partition}:frauddetector:\${Region}: \${Account}:detector-version/\${ResourcePath}	aws:ResourceTag/\${TagKey} (p. 914)
entity-type	arn:\${Partition}:frauddetector:\${Region}: \${Account}:entity-type/\${ResourcePath}	aws:ResourceTag/\${TagKey} (p. 914)

Resource types	ARN	Condition keys
external-model	arn:\${Partition}:frauddetector:\${Region}: \${Account}:external-model/\${ResourcePath}	aws:ResourceTag/ \${TagKey} (p. 914)
event-type	arn:\${Partition}:frauddetector:\${Region}: \${Account}:event-type/\${ResourcePath}	aws:ResourceTag/ \${TagKey} (p. 914)
label	arn:\${Partition}:frauddetector:\${Region}: \${Account}:label/\${ResourcePath}	aws:ResourceTag/ \${TagKey} (p. 914)
model	arn:\${Partition}:frauddetector:\${Region}: \${Account}:model/\${ResourcePath}	aws:ResourceTag/ \${TagKey} (p. 914)
model-version	arn:\${Partition}:frauddetector:\${Region}: \${Account}:model-version/\${ResourcePath}	aws:ResourceTag/ \${TagKey} (p. 914)
outcome	arn:\${Partition}:frauddetector:\${Region}: \${Account}:outcome/\${ResourcePath}	aws:ResourceTag/ \${TagKey} (p. 914)
rule	arn:\${Partition}:frauddetector:\${Region}: \${Account}:rule/\${ResourcePath}	aws:ResourceTag/ \${TagKey} (p. 914)
variable	arn:\${Partition}:frauddetector:\${Region}: \${Account}:variable/\${ResourcePath}	aws:ResourceTag/ \${TagKey} (p. 914)
batch-import	arn:\${Partition}:frauddetector:\${Region}: \${Account}:batch-import/\${ResourcePath}	aws:ResourceTag/ \${TagKey} (p. 914)

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 [Available global condition 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 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 \(p. 915\)](#)
- [Resource types defined by Amazon FreeRTOS \(p. 916\)](#)
- [Condition keys for Amazon FreeRTOS \(p. 916\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSoftwareConfiguration	Creates a software configuration	Write	configuration* (p. 916)		
				aws:RequestTag/\${TagKey} (p. 916)	
				aws:TagKeys (p. 916)	
DeleteSoftwareConfiguration	Deletes the software configuration	Write	configuration* (p. 916)		
DescribeHardwarePlatform	Describes the hardware platform	Read			
DescribeSoftwareConfiguration	Describes the software configuration	Read	configuration* (p. 916)		
GetSoftwareURL	Get the URL for Amazon FreeRTOS software download	Read			
GetSoftwareURLForFreeRTOSSoftware	Get the URL for Amazon FreeRTOS software download based on the configuration	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListFreeRTOSVersions	Lists versions of AmazonFreeRTOS	List			
ListHardwarePlatforms	Lists the hardware platforms	List			
ListHardwareVendors	Lists the hardware vendors	List			
ListSoftwareConfigurations	Lists the software configurations	List			
UpdateSoftwareConfiguration	Updates the software configuration	Write	configuration* (p. 916)		

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 \(p. 915\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
configuration	<code>arn:\${Partition}:freertos:\${Region}:\${Account}:configuration/\${ConfigurationName}</code>	aws:ResourceTag/\${TagKey} (p. 916)

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 [Available global condition keys](#).

Condition keys	Description	Type
aws:RequestTag/\${TagKey}	A tag key that is present in the request that the user makes to Amazon FreeRTOS	String
aws:ResourceTag/\${TagKey}	The tag key component of a tag attached to an Amazon FreeRTOS resource	String
aws:TagKeys	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 \(p. 917\)](#)
- [Resource types defined by Amazon FSx \(p. 923\)](#)
- [Condition keys for Amazon FSx \(p. 924\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("`**`") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateFileGateway	Grants permission to associate a File Gateway instance with an Amazon FSx for Windows File Server file system	Write	file-system* (p. 923)		
AssociateFileSystemDNSSuffixes	Grants permission to associate DNS suffixes with an Amazon FSx for Windows File Server file system	Write	file-system* (p. 923)		
CancelDataRepositoryTask	Grants permission to cancel a data repository task	Write	task* (p. 923)		
CopyBackup	Grants permission to copy a backup	Write	backup* (p. 923)		<code>fsx:TagResource</code>

Service Authorization Reference
Service Authorization Reference
Amazon FSx

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 924) aws:TagKeys (p. 924)	
CreateBackup	Grants permission to create a new backup of an Amazon FSx file system or an Amazon FSx volume	Write	backup* (p. 923) file-system (p. 923) volume (p. 923)	aws:RequestTag/ \${TagKey} (p. 924) aws:TagKeys (p. 924)	fsx:TagResource
CreateDataRepository	Grants permission to create a new Data repository association for an Amazon FSx for Lustre file system	Write	association* (p. 923) file-system* (p. 923)	aws:RequestTag/ \${TagKey} (p. 924) aws:TagKeys (p. 924)	fsx:TagResource
CreateDataRepository	Grants permission to create a new Data repository task for an Amazon FSx for Lustre file system	Write	file-system* (p. 923) task* (p. 923)	aws:RequestTag/ \${TagKey} (p. 924) aws:TagKeys (p. 924)	fsx:TagResource
CreateFileSystem	Grants permission to create a new, empty, Amazon FSx file system	Write	file-system* (p. 923)	aws:RequestTag/ \${TagKey} (p. 924) aws:TagKeys (p. 924)	fsx:TagResource
CreateFileSystem	Grants permission to create a New Amazon file system from an existing backup	Write	backup* (p. 923) file-system* (p. 923)	aws:RequestTag/ \${TagKey} (p. 924) aws:TagKeys (p. 924)	fsx:TagResource
CreateSnapshot	Grants permission to create a new snapshot on a volume	Write	snapshot* (p. 924)		fsx:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume* (p. 923)		
			aws:RequestTag/ \${TagKey} (p. 924)		
			aws:TagKeys (p. 924)		
CreateStorageVirtualMachine	Grants permission to create a new storage virtual machine in an Amazon FSx for Ontap file system	Write	file-system* (p. 923)		fsx:TagResource
			storage-virtual-machine* (p. 923)		
			aws:RequestTag/ \${TagKey} (p. 924)		
			aws:TagKeys (p. 924)		
CreateVolume	Grants permission to create a new volume	Write	volume* (p. 923)		fsx:TagResource
			snapshot (p. 924)		
			aws:RequestTag/ \${TagKey} (p. 924)		
			aws:TagKeys (p. 924)		
			fsx:StorageVirtualMachineId (p. 924)		
			fsx:ParentVolumeId (p. 924)		
CreateVolumeFromBackup	Grants permission to create a new volume from backup	Write	backup* (p. 923)		fsx:TagResource
			storage-virtual-machine* (p. 923)		
			volume* (p. 923)		
			aws:RequestTag/ \${TagKey} (p. 924)		
			aws:TagKeys (p. 924)		
			fsx:StorageVirtualMachineId (p. 924)		
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* (p. 923)		
DeleteDataRepositoryAssociation	Grants permission to delete a data repository association	Write	association* (p. 923)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteFileSystem	Grants permission to delete a file system, deleting its contents and any existing automatic backups of the file system	Write	file-system* (p. 923)		fsx>CreateBackup fsx:TagResource
	backup (p. 923)				
				aws:RequestTag/\${TagKey} (p. 924) aws:TagKeys (p. 924)	
DeleteSnapshot	Grants permission to delete a snapshot on a volume	Write	snapshot* (p. 924)		
DeleteStorageVirtualMachine	Grants permission to delete a virtual machine, deleting its contents	Write	storage-virtual-machine* (p. 923)		
DeleteVolume	Grants permission to delete a volume, deleting its contents and any existing automatic backups of the volume	Write	volume* (p. 923)		
backup (p. 923)					
			aws:RequestTag/\${TagKey} (p. 924) aws:TagKeys (p. 924) fsx:StorageVirtualMachineId (p. 924) fsx:ParentVolumeId (p. 924)		
DescribeAssociatedFileGateways	Grants permission to describe File Gateway instances associated with an Amazon FSx for Windows File Server file system	Read	file-system* (p. 923)		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeFileSystems	Grants permission to return the descriptions of all DNS aliases owned by your Amazon FSx for Windows File Server file system	Read	file-system* (p. 923)		
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			
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			
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			
DisassociateFileGateway	Grants permission to disassociate a File Gateway instance from an Amazon FSx for Windows File Server file system	Write	file-system* (p. 923)		
DisassociateFileSystems	Grants permission to disassociate file system aliases with an Amazon FSx for Windows File Server file system	Write	file-system* (p. 923)		
ListTagsForResource	Grants permission to list tags for an Amazon FSx resource	Read	association (p. 923)		

Service Authorization Reference
Service Authorization Reference
Amazon FSx

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume (p. 923)		
ManageBackupPrincipals	Grants permission to manage backup principal associations through AWS Backup	Permissions management	backup* (p. 923)		
ReleaseFileSystems	Grants permission to release file system V3 locks	Write	file-system* (p. 923)		
RestoreVolumeFromSnapshot	Grants permission to restore volume state from a snapshot	Write	snapshot* (p. 924) volume* (p. 923)		
TagResource	Grants permission to tag an Amazon FSx resource	Tagging	association (p. 923) backup (p. 923) file-system (p. 923) snapshot (p. 924) storage-virtual-machine (p. 923) task (p. 923) volume (p. 923) aws:TagKeys (p. 924) aws:RequestTag/\${TagKey} (p. 924)		
UntagResource	Grants permission to remove a tag from an Amazon FSx resource	Tagging	association (p. 923) backup (p. 923) file-system (p. 923) snapshot (p. 924) storage-virtual-machine (p. 923) task (p. 923) volume (p. 923) aws:TagKeys (p. 924)		
UpdateDataRepositoryAssociation	Grants permission to update data repository association configuration	Write	association* (p. 923)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateFileSystem	Grants permission to update file system configuration	Write	file-system* (p. 923)		
UpdateSnapshot	Grants permission to update snapshot configuration	Write	snapshot* (p. 924)		
UpdateStorageVirtualMachine	Grants permission to update storage virtual machine configuration	Write	storage-virtual-machine* (p. 923)		
UpdateVolume	Grants permission to update volume configuration	Write	volume* (p. 923)		
				fsx:StorageVirtualMachineId (p. 924)	
				fsx:ParentVolumeId (p. 924)	

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 \(p. 917\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 924)
backup	arn:\${Partition}:fsx:\${Region}: \${Account}:backup/\${BackupId}	aws:ResourceTag/ \${TagKey} (p. 924)
storage-virtual-machine	arn:\${Partition}:fsx:\${Region}: \${Account}:storage-virtual-machine/ \${FileSystemId}/\${StorageVirtualMachineId}	aws:ResourceTag/ \${TagKey} (p. 924)
task	arn:\${Partition}:fsx:\${Region}: \${Account}:task/\${TaskId}	aws:ResourceTag/ \${TagKey} (p. 924)
association	arn:\${Partition}:fsx:\${Region}: \${Account}:association/\${FileSystemId}/ \${DataRepositoryAssociationId}	aws:ResourceTag/ \${TagKey} (p. 924)
volume	arn:\${Partition}:fsx:\${Region}: \${Account}:volume/\${FileSystemId}/ \${VolumeId}	aws:ResourceTag/ \${TagKey} (p. 924)

Resource types	ARN	Condition keys
snapshot	arn:\${Partition}:fsx:\${Region}:\${Account}:snapshot/\${VolumeId}/ \${SnapshotId}	aws:ResourceTag/\${TagKey} (p. 924)

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 [Available global condition keys](#).

Condition keys	Description	Type
aws:RequestTag/\${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/\${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
fsx:IsBackupCopyDestForCopyBackup	Filters access by whether the backup is a destination backup for a CopyBackup operation	Bool
fsx:IsBackupCopySourceForCopyBackup	Filters access by whether the backup is a source backup for a CopyBackup operation	Bool
fsx:ParentVolumeId	Filters access by the containing parent volume for mutating volume operations	String
fsx:StorageVirtualMachineVolume	Filters access by the containing storage virtual machine for a volume for mutating volume operations	String

Actions, resources, and condition keys for Amazon GameLift

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

References:

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

Topics

- [Actions defined by Amazon GameLift \(p. 925\)](#)
- [Resource types defined by Amazon GameLift \(p. 933\)](#)
- [Condition keys for Amazon GameLift \(p. 933\)](#)

Actions defined by Amazon GameLift

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

The **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 933)		
CreateAlias	Grants permission to define a new alias for a fleet	Write		aws:RequestTag/\${TagKey} (p. 934) aws:TagKeys (p. 934)	
CreateBuild	Grants permission to create a new game build using files stored in an Amazon S3 bucket	Write		aws:RequestTag/\${TagKey} (p. 934) aws:TagKeys (p. 934)	
CreateFleet	Grants permission to create a new fleet of computing resources to run your game servers	Write		aws:RequestTag/\${TagKey} (p. 934) aws:TagKeys (p. 934)	
CreateFleetLocation	Grants permission to specify additional locations for a fleet	Write	fleet* (p. 933)		
CreateGameServer	Grants permission to create a new game server group, set up a corresponding Auto Scaling group, and launch instances to host game servers	Write		aws:RequestTag/\${TagKey} (p. 934) aws:TagKeys (p. 934)	
CreateGameSession	Grants permission to start a new game session on a specified fleet	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateGameSession	Grants permission to set up a new queue for processing game session placement requests	Write		aws:RequestTag/ \${TagKey} (p. 934) aws:TagKeys (p. 934)	
CreateMatchmakingRuleSet	Grants permission to create a new FlexMatch matchmaker	Write		aws:RequestTag/ \${TagKey} (p. 934) aws:TagKeys (p. 934)	
CreateMatchmakingRuleSet	Grants permission to create a new rule set for FlexMatch	Write		aws:RequestTag/ \${TagKey} (p. 934) aws:TagKeys (p. 934)	
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} (p. 934) aws:TagKeys (p. 934)	
CreateVpcPeeringConnection	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			
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* (p. 933)		
DeleteBuild	Grants permission to delete a game build	Write	build* (p. 933)		
DeleteFleet	Grants permission to delete an empty fleet	Write	fleet* (p. 933)		
DeleteFleetLocation	Grants permission to delete locations for a fleet	Write	fleet* (p. 933)		

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* (p. 933)		
DeleteGameSessionQueue	Grants permission to delete an existing game session queue	Write	gameSessionQueue* (p. 933)		
DeleteMatchmakingConfiguration	Grants permission to delete an existing FlexMatch matchmaker	Write	matchmakingConfiguration* (p. 933)		
DeleteMatchmakingRuleSet	Grants permission to delete an existing FlexMatch matchmaking rule set	Write	matchmakingRuleSet* (p. 933)		
DeleteScalingPolicy	Grants permission to delete a set of auto-scaling rules	Write	fleet* (p. 933)		
DeleteScript	Grants permission to delete a Realtime Servers script	Write	script* (p. 933)		
DeleteVpcPeeringAuthorization	Grants permission to cancel a VPC peering authorization	Write			
DeleteVpcPeeringConnection	Grants permission to remove a peering connection between VPCs	Write			
DeregisterGameServer	Grants permission to remove a game server from a game server group	Write	gameServerGroup* (p. 933)		
DescribeAlias	Grants permission to retrieve properties for an alias	Read	alias* (p. 933)		
DescribeBuild	Grants permission to retrieve properties for a game build	Read	build* (p. 933)		
DescribeEC2InstanceTypeLimits	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 setting for fleets	Read			
DescribeFleetEvents	Grants permission to retrieve entries from a fleet's event log	Read	fleet* (p. 933)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeFleetLocations	Grants permission to retrieve general properties, including statuses, for a fleet's locations	Read	fleet* (p. 933)		
DescribeFleetLocationCapacity	Grants permission to retrieve the current capacity setting for a fleet's location	Read	fleet* (p. 933)		
DescribeFleetLocationUtilization	Grants permission to retrieve utilization statistics for fleet's location	Read	fleet* (p. 933)		
DescribeFleetPortSettings	Grants permission to retrieve the incoming connection permissions for a fleet	Read	fleet* (p. 933)		
DescribeFleetUtilization	Grants permission to retrieve utilization statistics for fleets	Read			
DescribeGameServerProperties	Grants permission to retrieve properties for a game server	Read	gameServerGroup* (p. 933)		
DescribeGameServerGroupProperties	Grants permission to retrieve properties for a game server group	Read	gameServerGroup* (p. 933)		
DescribeGameServerStatus	Grants permission to retrieve the status of EC2 instances in a game server group	Read	gameServerGroup* (p. 933)		
DescribeGameSessionProperties	Grants permission to retrieve properties for game sessions in a fleet, including the protection policy	Read			
DescribeGameSessionDetails	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 fleet	Read	fleet* (p. 933)		
DescribeMatchmaking	Grants permission to retrieve details of matchmaking tickets	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeMatchmakers	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			
DescribeRuntimeConfigurations	Grants permission to retrieve the configuration for a fleet	Read	fleet* (p. 933)		
DescribeScalingPolicies	Grants permission to retrieve all scaling policies that are applied to a fleet	Read	fleet* (p. 933)		
DescribeScript	Grants permission to retrieve properties for a Realtime Servers script	Read	script* (p. 933)		
DescribeVpcPeeringAuthorizations	Grants permission to retrieve valid VPC peering authorizations	Read			
DescribeVpcPeeringDetails	Grants permission to retrieve details about active or pending VPC peering connections	Read			
GetGameSessionLogUrl	Grants permission to retrieve the URL of stored logs for a game session	Read			
GetInstanceAccess	Grants permission to request remote access to a specified fleet instance	Read	fleet* (p. 933)		
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			
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* (p. 933)		
ListScripts	Grants permission to retrieve properties for all Realtime Servers scripts in the current region	List			
ListTagsForResources	Grants permission to retrieve tags for GameLift resources	Read	alias (p. 933)		
			build (p. 933)		
			fleet (p. 933)		
			gameServerGroup (p. 933)		
			gameSessionQueue (p. 933)		
			matchmakingConfiguration (p. 933)		
			matchmakingRuleSet (p. 933)		
			script (p. 933)		
PutScalingPolicy	Grants permission to create or update a fleet auto-scaling policy	Write	fleet* (p. 933)		
RegisterGameServer	Grants permission to notify GameLift FleetIQ when a new game server is ready to host gameplay	Write	gameServerGroup* (p. 933)		
RequestUploadCredentials	Grants permission to retrieve fresh upload credentials to use when uploading a new game build	Read	build* (p. 933)		
ResolveAlias	Grants permission to retrieve the fleet ID associated with an alias	Read	alias* (p. 933)		
ResumeGameServer	Grants permission to reinstate suspended FleetIQ activity for a game server group	Write	gameServerGroup* (p. 933)		
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	fleet* (p. 933)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartGameSessionPlacement	Grants permission to send a game session placement request to a game session queue	Write	gameSessionQueue* (p. 933)		
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	fleet* (p. 933)		
StopGameSessionPlacement	Grants permission to cancel a game session placement request that is in progress	Write			
StopMatchmaking	Grants permission to cancel a matchmaking or match backfill request that is in progress	Write			
SuspendGameServerTemporarily	Grants permission to temporarily stop FleetIQ activity for a game server group	Write	gameServerGroup* (p. 933)		
TagResource	Grants permission to tag GameLift resources	Tagging	alias (p. 933)		
UntagResource	Grants permission to untag GameLift resources	Tagging	alias (p. 933)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			gameSessionQueue (p. 933) matchmakingConfiguration (p. 933) matchmakingRuleSet (p. 933) script (p. 933) aws:TagKeys (p. 934)		
UpdateAlias	Grants permission to update the properties of an existing alias	Write	alias* (p. 933)		
UpdateBuild	Grants permission to update an existing build's metadata	Write	build* (p. 933)		
UpdateFleetAttributes	Grants permission to update the general properties of an existing fleet	Write	fleet* (p. 933)		
UpdateFleetCapacity	Grants permission to adjust a fleet's capacity settings	Write	fleet* (p. 933)		
UpdateFleetPortSettings	Grants permission to adjust a fleet's port settings	Write	fleet* (p. 933)		
UpdateGameServer	Grants permission to change game server properties, health status, or utilization status	Write	gameServerGroup* (p. 933)		
UpdateGameServerProperties	Grants permission to update properties for game server group, including allowed instance types	Write	gameServerGroup* (p. 933)		
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* (p. 933)		
UpdateMatchmakingConfiguration	Grants permission to update properties of an existing FlexMatch matchmaking configuration	Write	matchmakingConfiguration* (p. 933)		
UpdateRuntimeConfiguration	Grants permission to update how server processes are configured on instances in an existing fleet	Write	fleet* (p. 933)		
UpdateScript	Grants permission to update the metadata and content of an existing Realtime Servers script	Write	script* (p. 933)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ValidateMatchmakingRuleSet	Grants permission to validate the syntax of a FlexMatch matchmaking rule set	Read			

Resource types defined by Amazon GameLift

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the [Actions table \(p. 925\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
<code>alias</code>	<code>arn:\${Partition}:gamelift:\${Region}::alias/\${AliasId}</code>	aws:ResourceTag/\${TagKey} (p. 934)
<code>build</code>	<code>arn:\${Partition}:gamelift:\${Region}::\${AccountId}:build/\${BuildId}</code>	aws:ResourceTag/\${TagKey} (p. 934)
<code>script</code>	<code>arn:\${Partition}:gamelift:\${Region}::\${AccountId}:script/\${ScriptId}</code>	aws:ResourceTag/\${TagKey} (p. 934)
<code>fleet</code>	<code>arn:\${Partition}:gamelift:\${Region}::\${Account}:fleet/\${FleetId}</code>	aws:ResourceTag/\${TagKey} (p. 934)
<code>gameSessionQueue</code>	<code>arn:\${Partition}:gamelift:\${Region}::\${Account}:gamesessionqueue/\${GameSessionQueueName}</code>	aws:ResourceTag/\${TagKey} (p. 934)
<code>matchmakingConfiguration</code>	<code>arn:\${Partition}:gamelift:\${Region}::\${Account}:matchmakingconfiguration/\${MatchmakingConfigurationName}</code>	aws:ResourceTag/\${TagKey} (p. 934)
<code>matchmakingRuleSet</code>	<code>arn:\${Partition}:gamelift:\${Region}::\${Account}:matchmakingruleset/\${MatchmakingRuleSetName}</code>	aws:ResourceTag/\${TagKey} (p. 934)
<code>gameServerGroup</code>	<code>arn:\${Partition}:gamelift:\${Region}::\${Account}:gameservergroup/\${GameServerGroupName}</code>	aws:ResourceTag/\${TagKey} (p. 934)

Condition keys for Amazon GameLift

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

To view the global condition keys that are available to all services, see [Available global condition 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 Amazon GameSparks

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

References:

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

Topics

- [Actions defined by Amazon GameSparks \(p. 934\)](#)
- [Resource types defined by Amazon GameSparks \(p. 938\)](#)
- [Condition keys for Amazon GameSparks \(p. 938\)](#)

Actions defined by Amazon GameSparks

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

The **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateGame	Grants permission to create a game	Write		aws:RequestTag/\${TagKey} (p. 938)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys (p. 938)	
CreateSnapshot	Grants permission to create a snapshot of a game	Write	game* (p. 938)		
			aws:RequestTag/ \${TagKey} (p. 938)		
			aws:TagKeys (p. 938)		
CreateStage	Grants permission to create a stage in a game	Write	game* (p. 938)		
			aws:RequestTag/ \${TagKey} (p. 938)		
			aws:TagKeys (p. 938)		
DeleteGame	Grants permission to delete a game	Write	game* (p. 938)		
			aws:RequestTag/ \${TagKey} (p. 938)		
DeleteStage	Grants permission to delete a stage from a game	Write	game* (p. 938)		
			stage* (p. 938)		
			aws:RequestTag/ \${TagKey} (p. 938)		
DisconnectPlayer	Grants permission to disconnect a player from the game runtime	Write	game* (p. 938)		
			stage* (p. 938)		
			aws:RequestTag/ \${TagKey} (p. 938)		
ExportSnapshot	Grants permission to export a snapshot of the game configuration	Write	game* (p. 938)		
			aws:RequestTag/ \${TagKey} (p. 938)		
GetExtension	Grants permission to get details about an extension	Read		aws:RequestTag/ \${TagKey} (p. 938)	
GetExtensionVersion	Grants permission to get details about an extension version	Read		aws:RequestTag/ \${TagKey} (p. 938)	
GetGame	Grants permission to get details about a game	Read	game* (p. 938)		
			aws:RequestTag/ \${TagKey} (p. 938)		
GetGameConfiguration	Grants permission to get the configuration for the game	Read	game* (p. 938)		
			aws:RequestTag/ \${TagKey} (p. 938)		
GetGeneratedCodeJob		Read	game* (p. 938)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to get details about a job that is generating code for a snapshot			aws:RequestTag/\${TagKey} (p. 938)	
GetPlayerConnectionStatus	Grants permission to get the status of a player connection	Read	game* (p. 938)		
			stage* (p. 938)		
				aws:RequestTag/\${TagKey} (p. 938)	
GetSnapshot	Grants permission to get a snapshot of the game	Read	game* (p. 938)		
				aws:RequestTag/\${TagKey} (p. 938)	
GetStage	Grants permission to get information about a stage	Read	game* (p. 938)		
			stage* (p. 938)		
				aws:RequestTag/\${TagKey} (p. 938)	
GetStageDeploymentInformation	Grants permission to get information about a stage deployment	Read	game* (p. 938)		
			stage* (p. 938)		
				aws:RequestTag/\${TagKey} (p. 938)	
ImportGameConfigurationSnapshot	Grants permission to import a snapshot of a game configuration	Write	game* (p. 938)		
				aws:RequestTag/\${TagKey} (p. 938)	
InvokeBackend	Grants permission to invoke backend services for a specific game	Write	game* (p. 938)		
			stage* (p. 938)		
				aws:RequestTag/\${TagKey} (p. 938)	
ListExtensionVersions	Grants permission to list the extension versions	List			
ListExtensions	Grants permission to list the extensions	List			
ListGames	Grants permission to list the games	List			
ListGeneratedCodeJobs	Grants permission to get a list of code generation jobs for a snapshot	List	game* (p. 938)		
				aws:RequestTag/\${TagKey} (p. 938)	
ListSnapshots	Grants permission to get a list of snapshot summaries for a game	List	game* (p. 938)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 938)	
ListStageDeployments	Grants permission to get a list of stage deployment summaries for a game	List	game* (p. 938)		
			stage* (p. 938)		
				aws:RequestTag/ \${TagKey} (p. 938)	
ListStages	Grants permission to get a list of stage summaries for a game	List	game* (p. 938)		
				aws:RequestTag/ \${TagKey} (p. 938)	
ListTagsForResource	Grants permission to list the tags associated with a resource	Read	game (p. 938)		
			stage (p. 938)		
StartGeneratedCodeJob	Grants permission to start an asynchronous process that generates client code for system-defined and custom messages	Write	game* (p. 938)		
				aws:RequestTag/ \${TagKey} (p. 938)	
StartStageDeployment	Grants permission to deploy a snapshot to a stage and creates a new game runtime	Write	game* (p. 938)		
			stage* (p. 938)		
				aws:RequestTag/ \${TagKey} (p. 938)	
TagResource	Grants permission to adds tags to a resource	Tagging	game (p. 938)		
			stage (p. 938)		
				aws:RequestTag/ \${TagKey} (p. 938)	
				aws:TagKeys (p. 938)	
UntagResource	Grants permission to remove tags from a resource	Tagging	game (p. 938)		
			stage (p. 938)		
UpdateGame	Grants permission to change the metadata of a game	Write	game* (p. 938)		
				aws:RequestTag/ \${TagKey} (p. 938)	
UpdateGameConfiguration	Grants permission to change the working copy of the game configuration	Write	game* (p. 938)		
				aws:RequestTag/ \${TagKey} (p. 938)	
UpdateSnapshot	Grants permission to update the metadata of a snapshot	Write	game* (p. 938)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ {\$TagKey} (p. 938)	
UpdateStage	Grants permission to update the metadata of a stage	Write	game* (p. 938)		
			stage* (p. 938)		
				aws:RequestTag/ {\$TagKey} (p. 938)	

Resource types defined by Amazon GameSparks

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the [Actions table \(p. 934\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
game	arn:\${Partition}:gamesparks:\${Region}: \${Account}:game/\${GameId}	aws:ResourceTag/ {\$TagKey} (p. 938)
stage	arn:\${Partition}:gamesparks:\${Region}: \${Account}:game/\${GameId}/stage/\${StageName}	aws:ResourceTag/ {\$TagKey} (p. 938)

Condition keys for Amazon GameSparks

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

To view the global condition keys that are available to all services, see [Available global condition 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	String

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 \(p. 939\)](#)
- [Resource types defined by AWS Global Accelerator \(p. 943\)](#)
- [Condition keys for AWS Global Accelerator \(p. 943\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddCustomRoutingVifToPrivateCloud	Grants permission to add a virtual private cloud (VPC) subnet endpoint to a custom routing accelerator endpoint group	Write	endpointgroup* (p. 943)		
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			
AllowCustomRoutingFromCustomTraffic	Grants permission to allows custom routing of user traffic to	Write	endpointgroup* (p. 943)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	a private destination IP:PORT in a specific VPC subnet				
CreateAccelerator	Grants permission to create a standard accelerator	Write		aws:RequestTag/\${TagKey} (p. 943) aws:TagKeys (p. 944)	
CreateCustomRoutingAccelerator	Grants permission to create a Custom Routing accelerator	Write		aws:RequestTag/\${TagKey} (p. 943) aws:TagKeys (p. 944)	
CreateCustomRoutingEndpointGroup	Grants permission to create an endpoint group for the specified listener for a custom routing accelerator	Write		listener* (p. 943)	
CreateCustomRoutingListener	Grants permission to create a listener to process inbound connections from clients to a custom routing accelerator	Write		accelerator* (p. 943)	
CreateEndpointGroup	Grants permission to add an endpoint group to a standard accelerator listener	Write		listener* (p. 943)	
CreateListener	Grants permission to add a listener to a standard accelerator	Write		accelerator* (p. 943)	
DeleteAccelerator	Grants permission to delete a standard accelerator	Write		accelerator* (p. 943)	
DeleteCustomRoutingAccelerator	Grants permission to delete a custom routing accelerator	Write		accelerator* (p. 943)	
DeleteCustomRoutingEndpointGroup	Grants permission to delete an endpoint group from a listener for a custom routing accelerator	Write		endpointgroup* (p. 943)	
DeleteCustomRoutingListener	Grants permission to delete a listener for a custom routing accelerator	Write		listener* (p. 943)	
DeleteEndpointGroup	Grants permission to delete an endpoint group associated with a standard accelerator listener	Write		endpointgroup* (p. 943)	
DeleteListener	Grants permission to delete a listener from a standard accelerator	Write		listener* (p. 943)	
DenyCustomRoutingTraffic	Grants permission to disallow custom routing of user traffic to a private destination IP:PORT in a specific VPC subnet	Write		endpointgroup* (p. 943)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeprovisionByoip	Grants permission to releases the specified address range that you provisioned for use with your accelerator through bring your own IP addresses (BYOIP)	Write			
DescribeAccelerators	Grants permissions to describe a standard accelerator	Read	accelerator* (p. 943)		
DescribeAcceleratorAttributes	Grants permission to describe a standard accelerator attributes	Read	accelerator* (p. 943)		
DescribeCustomRoutingAccelerators	Grants permission to describe a custom routing accelerator	Read	accelerator* (p. 943)		
DescribeCustomRoutingEndpointGroups	Grants permission to describe the attributes of a custom routing accelerator	Read	accelerator* (p. 943)		
DescribeCustomRoutingListeners	Grants permission to describe endpoint groups for a custom routing accelerator	Read	endpointgroup* (p. 943)		
DescribeCustomRoutingListenersForCustomRoutingAccelerators	Grants permission to describe listeners for a custom routing accelerator	Read	listener* (p. 943)		
DescribeEndpoints	Grants permission to describe a standard accelerator endpoint group	Read	endpointgroup* (p. 943)		
DescribeListener	Grants permission to describe a standard accelerator listener	Read	listener* (p. 943)		
ListAccelerators	Grants permission to list all standard accelerators	List			
ListByoipCidrs	Grants permission to list the BYOIP cidrs	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* (p. 943)		
ListCustomRoutingListeners	Grants permission to list the listeners for a custom routing accelerator	List	accelerator* (p. 943)		
ListCustomRoutingPortMappings	Grants permission to list the port mappings for a custom routing accelerator	List	accelerator* (p. 943)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListCustomRouting	Grants permission to list specific endpoint IP address (a destination address) in a subnet	List			
ListEndpointGroups	Grants permission to list all endpoint groups associated with a standard accelerator listener	List	listener* (p. 943)		
ListListeners	Grants permission to list all listeners associated with a standard accelerator	List	accelerator* (p. 943)		
ListTagsForResource	Grants permission to list tags for a globalaccelerator resource	Read	accelerator (p. 943)		
ProvisionByoipCidr	Grants permission to provisions an address range for use with your accelerator through bring your own IP addresses (BYOIP)	Write			
RemoveCustomRouting	Grants permission to remove virtual private cloud (VPC) subnet endpoints from a custom routing accelerator endpoint group	Write	endpointgroup* (p. 943)		
TagResource	Grants permission to add tags to a globalaccelerator resource	Tagging	accelerator (p. 943)		
				aws:RequestTag/\${TagKey} (p. 943)	
UntagResource	Grants permission to remove tags from a globalaccelerator resource	Tagging	accelerator (p. 943)		
				aws:TagKeys (p. 944)	
UpdateAccelerator	Grants permission to update a standard accelerator	Write	accelerator* (p. 943)		
UpdateAccelerator	Grants permission to update a standard accelerator attributes	Write	accelerator* (p. 943)		
UpdateCustomRouting	Grants permission to update a custom routing accelerator	Write	accelerator* (p. 943)		
UpdateCustomRouting	Grants permission to update the attributes for a custom routing accelerator	Write	accelerator* (p. 943)		
UpdateCustomRouting	Grants permission to update a listener for a custom routing accelerator	Write	listener* (p. 943)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateEndpointGroup	Grants permission to update an endpoint group on a standard accelerator listener	Write	endpointgroup* (p. 943)		
UpdateListener	Grants permission to update a listener on a standard accelerator	Write	listener* (p. 943)		
WithdrawByoipConfiguration	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 \(p. 939\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
accelerator	<code>arn:\${Partition}:globalaccelerator::\${Account}:accelerator/\${AcceleratorId}</code>	aws:ResourceTag/\${TagKey} (p. 943)
listener	<code>arn:\${Partition}:globalaccelerator::\${Account}:accelerator/\${AcceleratorId}/listener/\${ListenerId}</code>	aws:ResourceTag/\${TagKey} (p. 943)
endpointgroup	<code>arn:\${Partition}:globalaccelerator::\${Account}:accelerator/\${AcceleratorId}/listener/\${ListenerId}/endpoint-group/\${EndpointGroupId}</code>	aws:ResourceTag/\${TagKey} (p. 943)

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 [Available global condition keys](#).

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

Condition keys	Description	Type
aws:TagKeys	Filters actions based on the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for 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 \(p. 944\)](#)
- [Resource types defined by AWS Glue \(p. 958\)](#)
- [Condition keys for AWS Glue \(p. 959\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchCreatePartition	Grants permission to create one or more partitions	Write	catalog* (p. 958)		
			database* (p. 958)		
			table* (p. 958)		
BatchDeleteConnection	Grants permission to delete one or more connections	Write	catalog* (p. 958)		
			connection* (p. 958)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchDeletePartition	Grants permission to delete one or more partitions	Write	catalog* (p. 958)		
	database* (p. 958)				
	table* (p. 958)				
BatchDeleteTable	Grants permission to delete one or more tables	Write	catalog* (p. 958)		
	database* (p. 958)				
	table* (p. 958)				
BatchDeleteTableVersion	Grants permission to delete one or more versions of a table	Write	catalog* (p. 958)		
	database* (p. 958)				
	table* (p. 958)				
BatchGetBlueprints	Grants permission to retrieve one or more blueprints	Read	blueprint* (p. 959)		
BatchGetCrawlers	Grants permission to retrieve one or more crawlers	Read	crawler* (p. 959)		
BatchGetCustomEntityType	Grants permission to retrieve one or more Custom Entity Types	Read			
BatchGetDevEndpoints	Grants permission to retrieve one or more development endpoints	Read	devendpoint* (p. 958)		
BatchGetJobs	Grants permission to retrieve one or more jobs	Read	job* (p. 959)		
BatchGetPartitions	Grants permission to retrieve one or more partitions	Read	catalog* (p. 958)		
	database* (p. 958)				
	table* (p. 958)				
BatchGetTriggers	Grants permission to retrieve one or more triggers	Read	trigger* (p. 959)		
BatchGetWorkflows	Grants permission to retrieve one or more workflows	Read	workflow* (p. 959)		
BatchStopJobRun	Grants permission to stop one or more job runs for a job	Write	job* (p. 959)		
BatchUpdatePartitions	Grants permission to update one or more partitions	Write	catalog* (p. 958)		
	database* (p. 958)				
	table* (p. 958)				
CancelMLTaskRun	Grants permission to stop a running ML Task Run	Write	mlTransform* (p. 959)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelStatement	Grants permission to cancel a statement in an interactive session	Write	session* (p. 959)		
CheckSchemaVersion	Grants permission to retrieve schema validity of schema version	Read			
CreateBlueprint	Grants permission to create a blueprint	Write		aws:RequestTag/\${TagKey} (p. 959) aws:TagKeys (p. 959)	
CreateClassifier	Grants permission to create a classifier	Write			
CreateConnection	Grants permission to create a connection	Write	catalog* (p. 958)		
				aws:RequestTag/\${TagKey} (p. 959) aws:TagKeys (p. 959)	
CreateCrawler	Grants permission to create a crawler	Write			
CreateCustomEntityType	Grants permission to create a Custom Entity Type	Write			
CreateDatabase	Grants permission to create a database	Write	catalog* (p. 958)		
CreateDevEndpoint	Grants permission to create a development endpoint	Write		aws:RequestTag/\${TagKey} (p. 959) aws:TagKeys (p. 959)	
CreateJob	Grants permission to create a job	Write		aws:RequestTag/\${TagKey} (p. 959) aws:TagKeys (p. 959) glue:VpcIds (p. 960) glue:SubnetIds (p. 960) glue:SecurityGroupIds (p. 959)	
CreateMLTransform	Grants permission to create an ML Transform	Write		aws:RequestTag/\${TagKey} (p. 959) aws:TagKeys (p. 959)	
CreatePartition	Grants permission to create a partition	Write	catalog* (p. 958)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			database* (p. 958)		
			table* (p. 958)		
CreatePartitionIndex	Grants permission to create a specified partition index in an existing table	Write	catalog* (p. 958)		
			database* (p. 958)		
			table* (p. 958)		
CreateRegistry	Grants permission to create a new schema registry	Write	registry* (p. 959)		
				aws:RequestTag/\${TagKey} (p. 959)	
				aws:TagKeys (p. 959)	
CreateSchema	Grants permission to create a new schema container	Write	registry* (p. 959)		
			schema* (p. 959)		
				aws:RequestTag/\${TagKey} (p. 959)	
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		aws:RequestTag/\${TagKey} (p. 959)	
CreateTable	Grants permission to create a table	Write	catalog* (p. 958)		
			database* (p. 958)		
CreateTrigger	Grants permission to create a trigger	Write		aws:RequestTag/\${TagKey} (p. 959)	
				aws:TagKeys (p. 959)	
CreateUserDefinedFunction	Grants permission to create a function definition	Write	catalog* (p. 958)		
			database* (p. 958)		
CreateWorkflow	Grants permission to create a workflow	Write		aws:RequestTag/\${TagKey} (p. 959)	
				aws:TagKeys (p. 959)	
DeleteBlueprint	Grants permission to delete a blueprint	Write	blueprint* (p. 959)		

Service Authorization Reference
Service Authorization Reference
AWS Glue

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteClassifier	Grants permission to delete a classifier	Write			
DeleteColumnStatistics	Grants permission to delete the partition column statistics of a column	Write	catalog* (p. 958) database* (p. 958) table* (p. 958)		
DeleteColumnTableStatistics	Grants permission to delete the table statistics of columns	Write	catalog* (p. 958) database* (p. 958) table* (p. 958)		
DeleteConnection	Grants permission to delete a connection	Write	catalog* (p. 958) connection* (p. 958)		
DeleteCrawler	Grants permission to delete a crawler	Write	crawler* (p. 959)		
DeleteCustomEntityType	Grants permission to delete a Custom Entity Type	Write			
DeleteDatabase	Grants permission to delete a database	Write	catalog* (p. 958) database* (p. 958) table* (p. 958) userdefinedfunction* (p. 958)		
DeleteDevEndpoint	Grants permission to delete a development endpoint	Write	devendpoint* (p. 958)		
DeleteJob	Grants permission to delete a job	Write	job* (p. 959)		
DeleteMLTransform	Grants permission to delete an ML Transform	Write	mlTransform* (p. 959)		
DeletePartition	Grants permission to delete a partition	Write	catalog* (p. 958) database* (p. 958) table* (p. 958)		
DeletePartitionIndex	Grants permission to delete a specified partition index from an existing table	Write	catalog* (p. 958) database* (p. 958) table* (p. 958)		
DeleteRegistry	Grants permission to delete a schema registry	Write	registry* (p. 959)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteResourcePolicy	Grants permission to delete a resource policy	Permissions management	catalog* (p. 958)		
DeleteSchema	Grants permission to delete a schema container	Write	registry* (p. 959) schema* (p. 959)		
DeleteSchemaVersionRange	Grants permission to delete a range of schema versions	Write	registry* (p. 959) schema* (p. 959)		
DeleteSecurityConfiguration	Grants permission to delete a security configuration	Write			
DeleteSession	Grants permission to delete an interactive session after stopping the session if not already stopped	Write	session* (p. 959)		
DeleteTable	Grants permission to delete a table	Write	catalog* (p. 958)		
			database* (p. 958)		
			table* (p. 958)		
DeleteTableVersion	Grants permission to delete a version of a table	Write	catalog* (p. 958)		
			database* (p. 958)		
			table* (p. 958)		
DeleteTrigger	Grants permission to delete a trigger	Write	trigger* (p. 959)		
DeleteUserDefinedFunction	Grants permission to delete a function definition	Write	catalog* (p. 958)		
			database* (p. 958)		
			userdefinedfunction* (p. 958)		
DeleteWorkflow	Grants permission to delete a workflow	Write	workflow* (p. 959)		
GetBlueprint	Grants permission to retrieve a blueprint	Read	blueprint* (p. 959)		
GetBlueprintRun	Grants permission to retrieve a blueprint run	Read	blueprint* (p. 959)		
GetBlueprintRuns	Grants permission to retrieve all runs of a blueprint	Read	blueprint* (p. 959)		
GetCatalogImportStatus	Grants permission to retrieve the catalog import status	Read	catalog* (p. 958)		
GetClassifier	Grants permission to retrieve a classifier	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetClassifiers	Grants permission to list all classifiers	Read			
GetColumnStatistics	Grants permission to retrieve partition statistics of columns	Read	catalog* (p. 958) database* (p. 958) table* (p. 958)		
GetColumnStatistics	Grants permission to retrieve table statistics of columns	Read	catalog* (p. 958) database* (p. 958) table* (p. 958)		
GetConnection	Grants permission to retrieve a connection	Read	catalog* (p. 958) connection* (p. 958)		
GetConnections	Grants permission to retrieve a list of connections	Read	catalog* (p. 958) connection* (p. 958)		
GetCrawler	Grants permission to retrieve a crawler	Read	crawler* (p. 959)		
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			
GetDataCatalogEncryptionSettings	Grants permission to retrieve catalog encryption settings	Read	catalog* (p. 958)		
GetDatabase	Grants permission to retrieve a database	Read	catalog* (p. 958) database* (p. 958)		
GetDatabases	Grants permission to retrieve all databases	Read	catalog* (p. 958) database* (p. 958)		
GetDataflowGraph	Grants permission to transform a script into a directed acyclic graph (DAG)	Read			
GetDevEndpoint	Grants permission to retrieve a development endpoint	Read	devendpoint* (p. 958)		
GetDevEndpoints	Grants permission to retrieve all development endpoints	Read			
GetJob	Grants permission to retrieve a job	Read	job* (p. 959)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetJobBookmark	Grants permission to retrieve a job bookmark	Read			
GetJobRun	Grants permission to retrieve a job run	Read	job* (p. 959)		
GetJobRuns	Grants permission to retrieve all job runs of a job	Read	job* (p. 959)		
GetJobs	Grants permission to retrieve all current jobs	Read			
GetMLTaskRun	Grants permission to retrieve an ML Task Run	Read	mlTransform* (p. 959)		
GetMLTaskRuns	Grants permission to retrieve all ML Task Runs	List	mlTransform* (p. 959)		
GetMLTransform	Grants permission to retrieve an ML Transform	Read	mlTransform* (p. 959)		
GetMLTransforms	Grants permission to retrieve all ML Transforms	List	mlTransform* (p. 959)		
GetMapping	Grants permission to create a mapping	Read			
GetPartition	Grants permission to retrieve a partition	Read	catalog* (p. 958)		
			database* (p. 958)		
			table* (p. 958)		
GetPartitionIndex	Grants permission to retrieve partition indexes for a table	Read	catalog* (p. 958)		
			database* (p. 958)		
			table* (p. 958)		
GetPartitions	Grants permission to retrieve the partitions of a table	Read	catalog* (p. 958)		
			database* (p. 958)		
			table* (p. 958)		
GetPlan	Grants permission to retrieve a mapping for a script	Read			
GetRegistry	Grants permission to retrieve a schema registry	Read	registry* (p. 959)		
GetResourcePolicies	Grants permission to retrieve resource policies	Read	catalog* (p. 958)		
GetResourcePolicy	Grants permission to retrieve a resource policy	Read	catalog* (p. 958)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSchema	Grants permission to retrieve a schema container	Read	registry* (p. 959)		
			schema* (p. 959)		
GetSchemaByDefinition	Grants permission to retrieve a schema version based on schema definition	Read	registry* (p. 959)		
			schema* (p. 959)		
GetSchemaVersion	Grants permission to retrieve a schema version	Read	registry (p. 959)		
			schema (p. 959)		
GetSchemaVersions	Grants permission to compare two schema versions in schema registry	Read	registry* (p. 959)		
			schema* (p. 959)		
GetSecurityConfigurations	Grants permission to retrieve a security configuration	Read			
GetSecurityConfigs	Grants permission to retrieve one or more security configurations	Read			
GetSession	Grants permission to retrieve an interactive session	Read	session* (p. 959)		
GetStatement	Grants permission to retrieve result and information about a statement in an interactive session	Read	session* (p. 959)		
GetTable	Grants permission to retrieve a table	Read	catalog* (p. 958)		
			database* (p. 958)		
			table* (p. 958)		
GetTableVersion	Grants permission to retrieve a version of a table	Read	catalog* (p. 958)		
			database* (p. 958)		
			table* (p. 958)		
GetTableVersions	Grants permission to retrieve a list of versions of a table	Read	catalog* (p. 958)		
			database* (p. 958)		
			table* (p. 958)		
GetTables	Grants permission to retrieve the tables in a database	Read	catalog* (p. 958)		
			database* (p. 958)		
			table* (p. 958)		
GetTags	Grants permission to retrieve all tags associated with a resource	Read	blueprint (p. 959)		
			crawler (p. 959)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			devendpoint (p. 958)		
			job (p. 959)		
			trigger (p. 959)		
			workflow (p. 959)		
GetTrigger	Grants permission to retrieve a trigger	Read	trigger* (p. 959)		
GetTriggers	Grants permission to retrieve the triggers associated with a job	Read			
 GetUserDefinedFunction	Grants permission to retrieve a function definition	Read	catalog* (p. 958)		
	database* (p. 958)				
	userdefinedfunction* (p. 958)				
 GetUserDefinedFunctions	Grants permission to retrieve multiple function definitions	Read	catalog* (p. 958)		
	database* (p. 958)				
	userdefinedfunction* (p. 958)				
GetWorkflow	Grants permission to retrieve a workflow	Read	workflow* (p. 959)		
GetWorkflowRun	Grants permission to retrieve a workflow run	Read	workflow* (p. 959)		
	workflowrun properties				
GetWorkflowRuns	Grants permission to retrieve all runs of a workflow	Read	workflow* (p. 959)		
	workflowrun properties				
ImportCatalogToAthena	Grants permission to import an Athena data catalog into AWS Glue	Write	catalog* (p. 958)		
	athena catalog				
ListBlueprints	Grants permission to retrieve all blueprints	List		aws:RequestTag/ \${TagKey} (p. 959)	
ListCrawlers	Grants permission to retrieve all crawlers	List		aws:RequestTag/ \${TagKey} (p. 959)	
ListCustomEntityTypes	Grants permission to retrieve all Custom Entity Types	List		aws:RequestTag/ \${TagKey} (p. 959)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDevEndpoints	Grants permission to retrieve all development endpoints	List		aws:RequestTag/ \${TagKey} (p. 959)	
ListJobs	Grants permission to retrieve all current jobs	List		aws:RequestTag/ \${TagKey} (p. 959)	
ListMLTransforms	Grants permission to retrieve all ML Transforms	List	mlTransform* (p. 959)		
				aws:RequestTag/ \${TagKey} (p. 959)	aws:TagKeys (p. 959)
ListRegistries	Grants permission to retrieve a list of schema registries	List			
ListSchemaVersions	Grants permission to retrieve a list of schema versions	List	registry* (p. 959)		
				schema* (p. 959)	
ListSchemas	Grants permission to retrieve a list of schema containers	List	registry (p. 959)		
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* (p. 959)		
ListTriggers	Grants permission to retrieve all triggers	List		aws:RequestTag/ \${TagKey} (p. 959)	aws:TagKeys (p. 959)
ListWorkflows	Grants permission to retrieve all workflows	List			
NotifyEvent	Grants permission to notify an event to the event-driven workflow	Write	workflow* (p. 959)		
PutDataCatalogEncryptionSettings	Grants permission to update catalog encryption settings	Write	catalog* (p. 958)		
PutResourcePolicy	Grants permission to update a resource policy	Permissions management	catalog* (p. 958)		
PutSchemaVersionMetadata	Grants permission to add metadata to schema version		registry (p. 959)		schema (p. 959)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions	
PutWorkflowRunProperties	Grants permission to update <code>WorkflowRun</code> properties	Write	workflow* (p. 959)			
QuerySchemaVersionMetadata	Grants permission to fetch <code>schema</code> metadata for a schema version	List	registry (p. 959) schema (p. 959)			
RegisterSchemaVersion	Grants permission to create a new schema version	Write	registry* (p. 959) schema* (p. 959)			
RemoveSchemaVersionMetadata	Grants permission to remove schema version metadata from	Write	registry (p. 959) schema (p. 959)			
ResetJobBookmark	Grants permission to reset a job bookmark	Write				
ResumeWorkflowRun	Grants permission to resume a workflow run	Write	workflow* (p. 959)			
RunStatement	Grants permission to run a code or statement in an interactive session	Write	session* (p. 959)			
SearchTables	Grants permission to retrieve the tables in the catalog	Read	catalog* (p. 958) database* (p. 958) table* (p. 958)			
StartBlueprintRun	Grants permission to start running a blueprint		Write	blueprint* (p. 959)		
StartCrawler	Grants permission to start a crawler		Write	crawler* (p. 959)		
StartCrawlerSchedule	Grants permission to change the schedule state of a crawler to SCHEDULED	Write				
StartExportLabels	Grants permission to start an Export Labels ML Task Run	Write	mlTransform* (p. 959)			
StartImportLabels	Grants permission to start an Import Labels ML Task Run	Write	mlTransform* (p. 959)			
StartJobRun	Grants permission to start running a job	Write	job* (p. 959)			
StartMLEvaluation	Grants permission to start an Evaluation ML Task Run	Write	mlTransform* (p. 959)			
StartMLLabeling	Grants permission to start a Labeling Set Generation ML Task Run	Write	mlTransform* (p. 959)			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions	
StartTrigger	Grants permission to start a trigger	Write	trigger* (p. 959)			
StartWorkflowRun	Grants permission to start running a workflow	Write	workflow* (p. 959)			
StopCrawler	Grants permission to stop a running crawler	Write	crawler* (p. 959)			
StopCrawlerSchedule	Grants permission to set the schedule state of a crawler to NOT_SCHEDULED	Write				
StopSession	Grants permission to stop an interactive session	Write	session* (p. 959)			
StopTrigger	Grants permission to stop a trigger	Write	trigger* (p. 959)			
StopWorkflowRun	Grants permission to stop a workflow run	Write	workflow* (p. 959)			
TagResource	Grants permission to add tags to a resource	Tagging	blueprint (p. 959)			
				crawler (p. 959)		
				devendpoint (p. 958)		
				job (p. 959)		
				trigger (p. 959)		
				workflow (p. 959)		
				aws:TagKeys (p. 959)		
				aws:RequestTag/ \${TagKey} (p. 959)		
UntagResource	Grants permission to remove tags associated with a resource	Tagging	blueprint (p. 959)			
				crawler (p. 959)		
				devendpoint (p. 958)		
				job (p. 959)		
				trigger (p. 959)		
				workflow (p. 959)		
				aws:TagKeys (p. 959)		
				aws:RequestTag/ \${TagKey} (p. 959)		
UpdateBlueprint	Grants permission to update a blueprint	Write	blueprint* (p. 959)			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateClassifier	Grants permission to update a classifier	Write			
UpdateColumnStatistics	Grants permission to update partition statistics of columns	Write	catalog* (p. 958) database* (p. 958) table* (p. 958)		
UpdateColumnTableStatistics	Grants permission to update table statistics of columns	Write	catalog* (p. 958) database* (p. 958) table* (p. 958)		
UpdateConnection	Grants permission to update a connection	Write	catalog* (p. 958) connection* (p. 958)		
UpdateCrawler	Grants permission to update a crawler	Write	crawler* (p. 959)		
UpdateCrawlerSchedule	Grants permission to update the schedule of a crawler	Write			
UpdateDatabase	Grants permission to update a database	Write	catalog* (p. 958) database* (p. 958)		
UpdateDevEndpoint	Grants permission to update a development endpoint	Write	devendpoint* (p. 958)		
UpdateJob	Grants permission to update a job	Write	job* (p. 959) glue:VpcIds (p. 960) glue:SubnetIds (p. 960) glue:SecurityGroupIds (p. 959)		
UpdateMLTransform	Grants permission to update an ML Transform	Write	mlTransform* (p. 959)		
UpdatePartition	Grants permission to update a partition	Write	catalog* (p. 958) database* (p. 958) table* (p. 958)		
UpdateRegistry	Grants permission to update a schema registry	Write	registry* (p. 959)		
UpdateSchema	Grants permission to update a schema container	Write	registry* (p. 959) schema* (p. 959)		
UpdateTable	Grants permission to update a table	Write	catalog* (p. 958)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			database* (p. 958)		
			table* (p. 958)		
UpdateTrigger	Grants permission to update a trigger	Write	trigger* (p. 959)		
UpdateUserDefinedFunctionDefinition	Grants permission to update a function definition	Write	catalog* (p. 958)		
			database* (p. 958)		
			userdefinedfunction* (p. 958)		
UpdateWorkflow	Grants permission to update a workflow	Write	workflow* (p. 959)		
UseMLTransforms	Grants permission to use an ML Transform from within a Glue ETL Script	Write	mlTransform* (p. 959)		

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 \(p. 944\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
catalog	arn:\${Partition}:glue:\${Region}: \${Account}:catalog	
database	arn:\${Partition}:glue:\${Region}: \${Account}:database/\${DatabaseName}	
table	arn:\${Partition}:glue:\${Region}: \${Account}:table/\${DatabaseName}/ \${TableName}	
tableversion	arn:\${Partition}:glue:\${Region}: \${Account}:tableVersion/\${DatabaseName}/ \${TableName}/\${TableVersionName}	
connection	arn:\${Partition}:glue:\${Region}: \${Account}:connection/\${ConnectionName}	
userdefinedfunction	arn:\${Partition}:glue:\${Region}: \${Account}:userDefinedFunction/ \${DatabaseName}/\${UserDefinedFunctionName}	
devendpoint	arn:\${Partition}:glue:\${Region}: \${Account}:devEndpoint/\${DevEndpointName}	aws:ResourceTag/ \${TagKey} (p. 959)

Resource types	ARN	Condition keys
job	arn:\${Partition}:glue:\${Region}: \${Account}:job/\${JobName}	aws:ResourceTag/ \${TagKey} (p. 959)
trigger	arn:\${Partition}:glue:\${Region}: \${Account}:trigger/\${TriggerName}	aws:ResourceTag/ \${TagKey} (p. 959)
crawler	arn:\${Partition}:glue:\${Region}: \${Account}:crawler/\${CrawlerName}	aws:ResourceTag/ \${TagKey} (p. 959)
workflow	arn:\${Partition}:glue:\${Region}: \${Account}:workflow/\${WorkflowName}	aws:ResourceTag/ \${TagKey} (p. 959)
blueprint	arn:\${Partition}:glue:\${Region}: \${Account}:blueprint/\${BlueprintName}	aws:ResourceTag/ \${TagKey} (p. 959)
mlTransform	arn:\${Partition}:glue:\${Region}: \${Account}:mlTransform/\${TransformId}	aws:ResourceTag/ \${TagKey} (p. 959)
registry	arn:\${Partition}:glue:\${Region}: \${Account}:registry/\${RegistryName}	aws:ResourceTag/ \${TagKey} (p. 959)
schema	arn:\${Partition}:glue:\${Region}: \${Account}:schema/\${SchemaName}	aws:ResourceTag/ \${TagKey} (p. 959)
session	arn:\${Partition}:glue:\${Region}: \${Account}:session/\${SessionId}	aws:ResourceTag/ \${TagKey} (p. 959)

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 [Available global condition 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
glue:CredentialIssuingService	Filters access by the service from which the credentials of the request is issued	String
glue:RoleAssumedBy	Filters access by the service from which the credentials of the request is obtained by assuming the customer role	String
glue:SecurityGroupId	Filters access by the ID of security groups configured for the Glue job	ArrayOfString

Condition keys	Description	Type
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 \(p. 960\)](#)
- [Resource types defined by AWS Glue DataBrew \(p. 964\)](#)
- [Condition keys for AWS Glue DataBrew \(p. 964\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 964)		
CreateDataset	Grants permission to create a dataset	Write			aws:RequestTag/\${TagKey} (p. 964)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					aws:TagKeys (p. 965)
CreateProfileJob	Grants permission to create a profile job	Write		aws:RequestTag/\${TagKey} (p. 964) aws:TagKeys (p. 965)	
CreateProject	Grants permission to create a project	Write		aws:RequestTag/\${TagKey} (p. 964) aws:TagKeys (p. 965)	
CreateRecipe	Grants permission to create a recipe	Write		aws:RequestTag/\${TagKey} (p. 964) aws:TagKeys (p. 965)	
CreateRecipeJob	Grants permission to create a recipe job	Write		aws:RequestTag/\${TagKey} (p. 964) aws:TagKeys (p. 965)	
CreateRuleset	Grants permission to create a ruleset	Write		aws:RequestTag/\${TagKey} (p. 964) aws:TagKeys (p. 965)	
CreateSchedule	Grants permission to create a schedule	Write		aws:RequestTag/\${TagKey} (p. 964) aws:TagKeys (p. 965)	
DeleteDataset	Grants permission to delete a dataset	Write	Dataset* (p. 964)		
DeleteJob	Grants permission to delete a job	Write	Job* (p. 964)		
DeleteProject	Grants permission to delete a project	Write	Project* (p. 964)		
DeleteRecipeVersion	Grants permission to delete a recipe version	Write	Recipe* (p. 964)		
DeleteRuleset	Grants permission to delete a ruleset	Write	Ruleset* (p. 964)		
DeleteSchedule	Grants permission to delete a schedule	Write	Schedule* (p. 964)		
DescribeDataset	Grants permission to view details about a dataset	Read	Dataset* (p. 964)		
DescribeJob	Grants permission to view details about a job	Read	Job* (p. 964)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeJobRun	Grants permission to view details about job run for a given job	Read	Job* (p. 964)		
DescribeProject	Grants permission to view details about a project	Read	Project* (p. 964)		
DescribeRecipe	Grants permission to view details about a recipe	Read	Recipe* (p. 964)		
DescribeRuleset	Grants permission to view details about a ruleset	Read	Ruleset* (p. 964)		
DescribeSchedule	Grants permission to view details about a schedule	Read	Schedule* (p. 964)		
ListDatasets	Grants permission to list datasets in your account	Read			
ListJobRuns	Grants permission to list job runs for a given job	Read	Job* (p. 964)		
ListJobs	Grants permission to list jobs in your account	Read			
ListProjects	Grants permission to list projects in your account	Read			
ListRecipeVersion	Grants permission to list versions in your recipe	Read	Recipe* (p. 964)		
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 (p. 964)		
Job (p. 964)					
Project (p. 964)					
Recipe (p. 964)					
Ruleset (p. 964)					
Schedule (p. 964)					
PublishRecipe	Grants permission to publish a major version of a recipe	Write	Recipe* (p. 964)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendProjectSessionAction	Grants permission to submit an action to the interactive session for a project	Write	Project* (p. 964)		
StartJobRun	Grants permission to start running a job	Write	Job* (p. 964)		
StartProjectSession	Grants permission to start an interactive session for a project	Write	Project* (p. 964)		
StopJobRun	Grants permission to stop a job run for a job	Write	Job* (p. 964)		
TagResource	Grants permission to add tags to a resource	Tagging	Dataset (p. 964)		
			Job (p. 964)		
			Project (p. 964)		
			Recipe (p. 964)		
			Ruleset (p. 964)		
			Schedule (p. 964)		
			aws:RequestTag/\${TagKey} (p. 964)		
			aws:TagKeys (p. 965)		
UntagResource	Grants permission to remove tags associated with a resource	Tagging	Dataset (p. 964)		
			Job (p. 964)		
			Project (p. 964)		
			Recipe (p. 964)		
			Ruleset (p. 964)		
			Schedule (p. 964)		
			aws:TagKeys (p. 965)		
UpdateDataset	Grants permission to modify a dataset	Write	Dataset* (p. 964)		
UpdateProfileJob	Grants permission to modify a profile job	Write	Job* (p. 964)		
UpdateProject	Grants permission to modify a project	Write	Project* (p. 964)		
UpdateRecipe	Grants permission to modify a recipe	Write	Recipe* (p. 964)		
UpdateRecipeJob	Grants permission to modify a recipe job	Write	Job* (p. 964)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateRuleset	Grants permission to modify a ruleset	Write	Ruleset* (p. 964)		
UpdateSchedule	Grants permission to modify a schedule	Write	Schedule* (p. 964)		

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 \(p. 960\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
Project	<code>arn:\${Partition}:databrew:\${Region}: \${Account}:project/\${ResourceId}</code>	aws:ResourceTag/\${TagKey} (p. 964)
Dataset	<code>arn:\${Partition}:databrew:\${Region}: \${Account}:dataset/\${ResourceId}</code>	aws:ResourceTag/\${TagKey} (p. 964)
Ruleset	<code>arn:\${Partition}:databrew:\${Region}: \${Account}:ruleset/\${ResourceId}</code>	aws:ResourceTag/\${TagKey} (p. 964)
Recipe	<code>arn:\${Partition}:databrew:\${Region}: \${Account}:recipe/\${ResourceId}</code>	aws:ResourceTag/\${TagKey} (p. 964)
Job	<code>arn:\${Partition}:databrew:\${Region}: \${Account}:job/\${ResourceId}</code>	aws:ResourceTag/\${TagKey} (p. 964)
Schedule	<code>arn:\${Partition}:databrew:\${Region}: \${Account}:schedule/\${ResourceId}</code>	aws:ResourceTag/\${TagKey} (p. 964)

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 [Available global condition 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 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 \(p. 965\)](#)
- [Resource types defined by AWS Ground Station \(p. 967\)](#)
- [Condition keys for AWS Ground Station \(p. 968\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 968)		
CreateConfig	Grants permission to create a configuration	Write		aws:RequestTag/\${TagKey} (p. 968) aws:TagKeys (p. 968)	

Service Authorization Reference
Service Authorization Reference
AWS Ground Station

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDataflowEndpointGroup	Grants permission to create a Dataflow endpoint group	Write		aws:RequestTag/ \${TagKey} (p. 968) aws:TagKeys (p. 968)	
CreateMissionProfile	Grants permission to create a Mission profile	Write		aws:RequestTag/ \${TagKey} (p. 968) aws:TagKeys (p. 968)	
DeleteConfig	Grants permission to delete a config	Write	Config* (p. 967)		
DeleteDataflowEndpointGroup	Grants permission to delete a Dataflow endpoint group	Write	DataflowEndpointGroup* (p. 968)		
DeleteMissionProfile	Grants permission to delete a Mission profile	Write	MissionProfile* (p. 968)		
DescribeContact	Grants permission to describe a contact	Read	Contact* (p. 968)		
GetConfig	Grants permission to return a configuration	Read	Config* (p. 967)		
GetDataflowEndpointGroup	Grants permission to return a Dataflow endpoint group	Read	DataflowEndpointGroup* (p. 968)		
GetMinuteUsage	Grants permission to return minutes usage	Read			
GetMissionProfile	Grants permission to retrieve a mission profile	Read	MissionProfile* (p. 968)		
GetSatellite	Grants permission to return information about a satellite	Read	Satellite* (p. 968)		
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 dataflow endpoint groups	List			
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 (p. 967)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Contact (p. 968)		
			DataflowEndpointGroup (p. 968)		
			MissionProfile (p. 968)		
ReserveContact	Grants permission to reserve a contact	Write		aws:RequestTag/\${TagKey} (p. 968) aws:TagKeys (p. 968)	
TagResource	Grants permission to assign a resource tag	Tagging	Config (p. 967)		
Contact (p. 968)					
DataflowEndpointGroup (p. 968)					
MissionProfile (p. 968)					
	aws:TagKeys (p. 968)				
UntagResource	Grants permission to deassign a resource tag	Tagging	Config (p. 967)		
Contact (p. 968)					
DataflowEndpointGroup (p. 968)					
MissionProfile (p. 968)					
	aws:TagKeys (p. 968)				
UpdateConfig	Grants permission to update a configuration	Write	Config* (p. 967)		
UpdateMissionProfile	Grants permission to update a mission profile	Write	MissionProfile* (p. 968)		

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 \(p. 965\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 968) groundstation:ConfigId (p. 968)

Resource types	ARN	Condition keys
		groundstation:ConfigType (p. 968)
Contact	arn:\${Partition}:groundstation:\${Region}: \${Account}:contact/\${ContactId}	aws:ResourceTag/ \${TagKey} (p. 968) groundstation:ContactId (p. 968)
DataflowEndpointGroup	arn:\${Partition}:groundstation:\${Region}: \${Account}:dataflow-endpoint-group/ \${DataflowEndpointGroupId}	aws:ResourceTag/ \${TagKey} (p. 968) groundstation:DataflowEndpointGroup
GroundStationResource	arn:\${Partition}:groundstation:\${Region}: \${Account}:groundstation:\${GroundStationId}	groundstation:GroundStationId (p. 968)
MissionProfile	arn:\${Partition}:groundstation: \${Region}: \${Account}:mission-profile/ \${MissionProfileId}	aws:ResourceTag/ \${TagKey} (p. 968) groundstation:MissionProfileId (p. 969)
Satellite	arn:\${Partition}:groundstation:\${Region}: \${Account}:satellite/\${SatelliteId}	groundstation:SatelliteId (p. 969)

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 [Available global condition 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
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
groundstation:GroundStationId	Filters access by the ID of a ground station	String

Condition keys	Description	Type
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 \(p. 969\)](#)
- [Resource types defined by Amazon GroundTruth Labeling \(p. 970\)](#)
- [Condition keys for Amazon GroundTruth Labeling \(p. 970\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociatePatchTemplateWithManifestFile [permission only]	Grants permission to associate a patch template with the manifest file to update the manifest file	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeConsoleJob [permission only]	Grants permission to get status of GroundTruthLabeling Jobs	Read			
ListDatasetObjects [permission only]	Grants permission to list dataset objects in a manifest file	Read			
RunFilterOrSampleRecords [permission only]	Grants permission to filter records from a manifest file using S3 select. Get sample entries based on random sampling	Write			
RunGenerateManifests [permission only]	Grants permission to list a S3 prefix and generate manifest files from objects in that location	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 [Available keys for conditions](#).

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 \(p. 971\)](#)
- [Resource types defined by Amazon GuardDuty \(p. 976\)](#)
- [Condition keys for Amazon GuardDuty \(p. 976\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 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} (p. 976) aws:TagKeys (p. 976)	
CreateFilter	Grants permission to create GuardDuty filters. A filter defines finding attributes and conditions used to filter findings	Write	filter* (p. 976)		
				aws:RequestTag/\${TagKey} (p. 976) aws:TagKeys (p. 976)	
CreateIPSet	Grants permission to create an IPSet	Write		aws:RequestTagDeleteRolePolicy/\${TagKey} (p. 976) iam:PutRolePolicy aws:TagKeys (p. 976)	
CreateMembers	Grants permission to create GuardDuty member accounts, where the account used to create a member becomes the GuardDuty administrator account	Write			
CreatePublishingDestination	Grants permission to create a publishing destination	Write			s3:GetObject s3>ListBucket
CreateSampleFindings	Grants permission to create sample findings	Write			

Service Authorization Reference
Service Authorization Reference
Amazon GuardDuty

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateThreatIntelSet	Grants permission to create GuardDuty ThreatIntelSets, where a ThreatIntelSet consists of known malicious IP addresses used by GuardDuty to generate findings	Write		aws:RequestTag/ \${TagKey} (p. 976) aws:TagKeys (p. 976)	
DeclineInvitation	Grants permission to decline invitations to become a GuardDuty member account	Write			
DeleteDetector	Grants permission to delete GuardDuty detectors	Write	detector* (p. 976)		
DeleteFilter	Grants permission to delete GuardDuty filters	Write	filter* (p. 976)		
DeleteIPSet	Grants permission to delete GuardDuty IPSets	Write	ipset* (p. 976)		
DeleteInvitations	Grants permission to delete invitations to become a GuardDuty member account	Write			
DeleteMembers	Grants permission to delete GuardDuty member accounts	Write			
DeletePublishingDestination	Grants permission to delete a publishing destination	Write	publishingDestination* (p. 976)		
DeleteThreatIntelSet	Grants permission to delete GuardDuty ThreatIntelSets	Write	threatintelset* (p. 976)		
DescribeOrganizationDelegatedAdministrator	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* (p. 976)		
DisableOrganizationDelegatedAdministrator	Grants permission to disable the organization delegated administrator for GuardDuty	Write			
DisassociateFromGuardDutyAdministratorAccount	Grants permission to disassociate a GuardDuty member account from its GuardDuty administrator account	Write			

Service Authorization Reference
Service Authorization Reference
Amazon GuardDuty

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateMembers	Grants permission to disassociate GuardDuty member accounts from their administrator GuardDuty account	Write			
EnableOrganization	Grants permission to enable an organization delegated administrator for GuardDuty	Write			
GetDetector	Grants permission to retrieve GuardDuty detectors	Read	detector* (p. 976)		
GetFilter	Grants permission to retrieve GuardDuty filters	Read	filter* (p. 976)		
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* (p. 976)		
GetInvitationsCount	Grants permission to retrieve the count of all GuardDuty invitations sent to a specified account, which does not include the accepted invitation	Read			
GetMasterAccount	Grants permission to retrieve details of the GuardDuty administrator account associated with a member account	Read			
GetMemberDetectors	Grants permission to describe which data sources are enabled for member accounts detectors	Read			
GetMembers	Grants permission to retrieve the member accounts associated with an administrator account	Read			
GetThreatIntelSet	Grants permission to retrieve GuardDuty ThreatIntelSets	Read	threatintelset* (p. 976)		
GetUsageStatistics	Grants permission to list Amazon GuardDuty usage statistics over the last 30 days for the specified detector ID	Read			

Service Authorization Reference
Service Authorization Reference
Amazon GuardDuty

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
InviteMembers	Grants permission to invite other AWS accounts to enable GuardDuty and become GuardDuty member accounts	Write			
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			
ListMembers	Grants permission to retrieve a list of GuardDuty member accounts associated with an administrator account	List			
ListOrganizationDetails	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 (p. 976)		
			filter (p. 976)		
			ipset (p. 976)		
			threatintelset (p. 976)		
ListThreatIntelSets	Grants permission to retrieve a list of GuardDuty ThreatIntelSets	List			
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			

Service Authorization Reference
Service Authorization Reference
Amazon GuardDuty

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to add tags to a GuardDuty resource	Tagging	detector (p. 976) filter (p. 976) ipset (p. 976) threatintelset (p. 976)		
	aws:RequestTag/ \${TagKey} (p. 976)				
	aws:TagKeys (p. 976)				
UnarchiveFinding	Grants permission to unarchive GuardDuty findings	Write			
UntagResource	Grants permission to remove tags from a GuardDuty resource	Tagging	detector (p. 976) filter (p. 976) ipset (p. 976) threatintelset (p. 976)		
	aws:TagKeys (p. 976)				
UpdateDetector	Grants permission to update GuardDuty detectors	Write	detector* (p. 976)		
UpdateFilter	Grants permission to updates GuardDuty filters	Write	filter* (p. 976)		
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* (p. 976)		iam:DeleteRolePolicy iam:PutRolePolicy
UpdateMemberDetector	Grants permission to update data sources are enabled for member accounts detectors	Write			
UpdateOrganizationDetector	Grants permission to update the delegated administrator configuration associated with a GuardDuty detector	Write			
UpdatePublishingDestination	Grants permission to update a Publishing destination	Write	publishingDestination* (p. 976) s3:GetObject s3>ListBucket		
UpdateThreatIntelSet	Grants permission to updates the GuardDuty ThreatIntelSets	Write	threatintelset* (p. 976)		iam:DeleteRolePolicy iam:PutRolePolicy

Resource types defined by Amazon GuardDuty

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the [Actions table \(p. 971\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
detector	<code>arn:\${Partition}:guardduty:\${Region}:\${Account}:detector/\${DetectorId}</code>	aws:ResourceTag/\${TagKey} (p. 976)
filter	<code>arn:\${Partition}:guardduty:\${Region}:\${Account}:detector/\${DetectorId}/filter/\${FilterName}</code>	aws:ResourceTag/\${TagKey} (p. 976)
ipset	<code>arn:\${Partition}:guardduty:\${Region}:\${Account}:detector/\${DetectorId}/ipset/\${IPSetId}</code>	aws:ResourceTag/\${TagKey} (p. 976)
threatintelset	<code>arn:\${Partition}:guardduty:\${Region}:\${Account}:detector/\${DetectorId}/threatintelset/\${ThreatIntelSetId}</code>	aws:ResourceTag/\${TagKey} (p. 976)
publishingDestination	<code>arn:\${Partition}:guardduty:\${Region}:\${Account}:detector/\${DetectorId}/publishingDestination/\${PublishingDestinationId}</code>	

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters access by tag key-value pairs in the request	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters access by tag key-value pairs attached to the resource	String
<code>aws:TagKeys</code>	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 \(p. 977\)](#)
- [Resource types defined by AWS Health APIs and Notifications \(p. 978\)](#)
- [Condition keys for AWS Health APIs and Notifications \(p. 979\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeAffectedAccounts	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* (p. 979)		
				health:eventTypeCode (p. 979)	health:service (p. 979)
DescribeAffectedEvents	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			
DescribeEventAggregates	Grants permission to retrieve the number of events of each event	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	type (issue, scheduled change, and account notification)				
DescribeEventDetails	Grants permission to retrieve detailed information about one or more specified events	Read	event* (p. 979)		
				health:eventTypeCode (p. 979)	
	health:service (p. 979)				
DescribeEventDetailsForOrganization	Grants permission to retrieve detailed information about one or more specified events for provided accounts in organization	Read			organizations>ListAccounts
DescribeEventTypes	Grants permission to retrieve the event types that meet the specified filter criteria	Read			
DescribeEvents	Grants permission to retrieve information about events that meet the specified filter criteria	Read			
DescribeEventsForOrganization	Grants permission to retrieve information about events that meet the specified filter criteria in organization	Read			organizations>ListAccounts
DescribeHealthServices	Grants permission to retrieve the states of enabling or disabling the Organizational View feature	Read			organizations>ListAccounts
DisableHealthService	Grants permission to disable the Organizational View feature	Permissions management			organizations>DisableAWSOrganizationalView
EnableHealthService	Grants permission to enable the Organizational View feature	Permissions management			iam>CreateServiceLinkedRole organizations>EnableAWSOrganizationalView 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 \(p. 977\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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}/\${EventCharCode}/*	

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 [Available global condition keys](#).

Condition keys	Description	Type
health:eventTypeCode	Filters access by event type	String
health:service	Filters access by impacted service	String

Actions, resources, and condition keys for Amazon HealthLake

Amazon 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 Amazon HealthLake \(p. 979\)](#)
- [Resource types defined by Amazon HealthLake \(p. 981\)](#)
- [Condition keys for Amazon HealthLake \(p. 982\)](#)

Actions defined by Amazon 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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your

policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateFHIRDatastore	Grants permission to create a datastore that can ingest and export FHIR data	Write		aws:RequestTag/\${TagKey} (p. 982) aws:TagKeys (p. 982)	
CreateResource	Grants permission to create resource	Write	datastore* (p. 981)		
DeleteFHIRDatastore	Grants permission to delete a datastore	Write	datastore* (p. 981)		
DeleteResource	Grants permission to delete resource	Write	datastore* (p. 981)		
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* (p. 981)		
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* (p. 981)		
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* (p. 981)		
GetCapabilities	Grants permission to get the capabilities of a FHIR datastore	Read	datastore* (p. 981)		
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* (p. 981)		
ListFHIRImportJobs	Grants permission to get a list of import jobs for the specified datastore	List	datastore* (p. 981)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResources	Grants permission to get a list of tags for the specified datastore	Read	datastore (p. 981)		
ReadResource	Grants permission to read resource	Read	datastore* (p. 981)		
SearchWithGet	Grants permission to search resources with GET method	Read	datastore* (p. 981)		
SearchWithPost	Grants permission to search resources with POST method	Read	datastore* (p. 981)		
StartFHIRExportJob	Grants permission to begin a FHIR Export job	Write	datastore* (p. 981)		
StartFHIRImportJob	Grants permission to begin a FHIR Import job	Write	datastore* (p. 981)		
TagResource	Grants permission to add tags to a datastore	Tagging	datastore (p. 981)		
			aws:TagKeys (p. 982)		
			aws:RequestTag/ \${TagKey} (p. 982)		
			aws:ResourceTag/ \${TagKey} (p. 982)		
UntagResource	Grants permission to remove tags associated with a datastore	Tagging	datastore (p. 981)		
			aws:TagKeys (p. 982)		
UpdateResource	Grants permission to update resource	Write	datastore* (p. 981)		

Resource types defined by Amazon 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 \(p. 979\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
datastore	<code>arn:\${Partition}:healthlake:\${Region}: \${AccountId}:datastore/fhir/\${DatastoreId}</code>	aws:ResourceTag/ \${TagKey} (p. 982)

Condition keys for Amazon HealthLake

Amazon 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 [Available global condition 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 High-volume outbound communications

High-volume outbound communications (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 High-volume outbound communications \(p. 982\)](#)
- [Resource types defined by High-volume outbound communications \(p. 984\)](#)
- [Condition keys for High-volume outbound communications \(p. 984\)](#)

Actions defined by High-volume outbound communications

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

The **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 984)		
			aws:TagKeys (p. 985)		
			aws:RequestTag/\${TagKey} (p. 985)		
DeleteCampaign	Grants permission to delete a campaign	Write	campaign* (p. 984)		
DescribeCampaign	Grants permission to describe a specific campaign	Read	campaign* (p. 984)		
			aws:RequestTag/\${TagKey} (p. 985)		
GetCampaignState	Grants permission to get state of a campaign	Read	campaign* (p. 984)		
			aws:RequestTag/\${TagKey} (p. 985)		
GetCampaignStates	Grants permission to get state of campaigns	Read	campaign* (p. 984)		
			aws:RequestTag/\${TagKey} (p. 985)		
ListCampaigns	Grants permission to provide summary of all campaigns	List		aws:RequestTag/\${TagKey} (p. 985)	
ListTagsForResource	Grants permission to list tags for a resource	Read	campaign (p. 984)		
			aws:ResourceTag/\${TagKey} (p. 985)		
PauseCampaign	Grants permission to pause a campaign	Write	campaign* (p. 984)		
PutConnectInstanceConfig	Grants permission to add configuration information for an Amazon Connect instance	Write			
PutDialRequestBatch	Grants permission to create dial requests for the specified campaign	Write	campaign* (p. 984)		
ResumeCampaign	Grants permission to resume a campaign	Write	campaign* (p. 984)		
StartCampaign	Grants permission to start a campaign	Write	campaign* (p. 984)		
StopCampaign	Grants permission to stop a campaign	Write	campaign* (p. 984)		
TagResource	Grants permission to tag a resource	Tagging	campaign (p. 984)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys (p. 985) aws:RequestTag/ {\$TagKey} (p. 985)	
UntagResource	Grants permission to untag a resource	Tagging	campaign (p. 984)		
				aws:TagKeys (p. 985) aws:RequestTag/ {\$TagKey} (p. 985)	
UpdateCampaign	Grants permission to update The id of configuration of a campaign	Write	campaign* (p. 984)		
UpdateCampaign	Grants permission to update the Name of a campaign	Write	campaign* (p. 984)		
UpdateCampaign	Grants permission to update the Outbound Call configuration of a campaign	Write	campaign* (p. 984)		

Resource types defined by High-volume outbound communications

The following resource types are defined by this service and can be used in the Resource element of IAM permission policy statements. Each action in the [Actions table \(p. 982\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 985)

Condition keys for High-volume outbound communications

High-volume outbound communications defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see [Condition keys table](#).

To view the global condition keys that are available to all services, see [Available global condition keys](#).

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

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 \(p. 985\)](#)
- [Resource types defined by Amazon Honeycode \(p. 988\)](#)
- [Condition keys for Amazon Honeycode \(p. 988\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 association request for your AWS Account	Write			
BatchCreateTableRows	Grants permission to create new rows in a table	Write	table* (p. 988)		
BatchDeleteTableRows	Grants permission to delete rows from a table	Write	table* (p. 988)		
BatchUpdateTableRows	Grants permission to update rows in a table	Write	table* (p. 988)		
BatchUpsertTableRows	Grants permission to upsert rows in a table	Write	table* (p. 988)		
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 [permission only]	Grants permission to remove groups from an Amazon Honeycode team for your AWS Account	Write			
DescribeTableDataImportJob	Grants permission to get details about a table data import job	Read	table* (p. 988)		
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* (p. 988)		
InvokeScreenAutomation	Grants permission to invoke a screen automation	Write	screen-automation* (p. 988)		
ListDomains [permission only]	Grants permission to list all Amazon Honeycode domains and their verification status for your AWS Account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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* (p. 988)		
ListTableRows	Grants permission to list the rows in a table	List	table* (p. 988)		
ListTables	Grants permission to list the tables in a workbook	List	workbook* (p. 988)		
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* (p. 988)		
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			
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			
StartTableDataImport	Grants permission to start a table data import job	Write	table* (p. 988)		
TagResource	Grants permission to tag a resource	Tagging			
UntagResource	Grants permission to untag a resource	Tagging			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 \(p. 985\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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 [Available keys for conditions](#).

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 \(p. 989\)](#)
- [Resource types defined by AWS IAM Access Analyzer \(p. 991\)](#)
- [Condition keys for AWS IAM Access Analyzer \(p. 991\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 991)		
CancelPolicyGeneration	Grants permission to cancel a policy generation	Write			
CreateAccessPreview	Grants permission to create an access preview for the specified analyzer	Write	Analyzer* (p. 991)		
CreateAnalyzer	Grants permission to create an analyzer	Write	Analyzer* (p. 991) aws:RequestTag/\${TagKey} (p. 992) aws:TagKeys (p. 992)		iam>CreateServiceLinkedRole
CreateArchiveRule	Grants permission to create an archive rule for the specified analyzer	Write	ArchiveRule* (p. 991)		
DeleteAnalyzer	Grants permission to delete the specified analyzer	Write	Analyzer* (p. 991)		
DeleteArchiveRule	Grants permission to delete archive rules for the specified analyzer	Write	ArchiveRule* (p. 991)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAccessPreview	Grants permission to retrieve information about an access preview	Read	Analyzer* (p. 991)		
GetAnalyzedResource	Grants permission to retrieve information about an analyzed resource	Read	Analyzer* (p. 991)		
GetAnalyzer	Grants permission to retrieve information about analyzers	Read	Analyzer* (p. 991)		
				aws:RequestTag/\${TagKey} (p. 992) aws:TagKeys (p. 992)	
GetArchiveRule	Grants permission to retrieve information about archive rules for the specified analyzer	Read	ArchiveRule* (p. 991)		
GetFinding	Grants permission to retrieve findings	Read	Analyzer* (p. 991)		
GetGeneratedPolicy	Grants permission to retrieve a policy that was generated using StartPolicyGeneration	Read			
ListAccessPreview	Grants permission to retrieve a list of findings from an access preview	Read	Analyzer* (p. 991)		
ListAccessPreviews	Grants permission to retrieve a list of access previews	List	Analyzer* (p. 991)		
ListAnalyzedResources	Grants permission to retrieve a list of resources that have been analyzed	Read	Analyzer* (p. 991)		
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* (p. 991)		
ListFindings	Grants permission to retrieve a list of findings from an analyzer	Read	Analyzer* (p. 991)		
ListPolicyGenerations	Grants permission to list all the recently started policy generations	Read			
ListTagsForResource	Grants permission to retrieve a list of tags applied to a resource	Read	Analyzer (p. 991)		
StartPolicyGeneration	Grants permission to start a policy generation	Write			iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartResourceScan	Grants permission to start a scan of the policies applied to a resource	Write	Analyzer* (p. 991)		
TagResource	Grants permission to add a tag to a resource	Tagging	Analyzer (p. 991)		
				aws:RequestTag/\${TagKey} (p. 992) aws:TagKeys (p. 992)	
UntagResource	Grants permission to remove a tag from a resource	Tagging	Analyzer (p. 991)		
				aws:RequestTag/\${TagKey} (p. 992) aws:TagKeys (p. 992)	
UpdateArchiveRule	Grants permission to modify an archive rule	Write	ArchiveRule* (p. 991)		
UpdateFindings	Grants permission to modify findings	Write	Analyzer* (p. 991)		
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](#) (p. 989) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
Analyzer	<code>arn:\${Partition}:access-analyzer:\${Region}:\${Account}:analyzer/\${AnalyzerName}</code>	aws:ResourceTag/\${TagKey} (p. 992)
ArchiveRule	<code>arn:\${Partition}:access-analyzer:\${Region}:\${Account}:analyzer/\${AnalyzerName}/archive-rule/\${RuleName}</code>	

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 [Available global condition 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 Identity And Access Management

Identity And Access Management (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 Identity And Access Management \(p. 992\)](#)
- [Resource types defined by Identity And Access Management \(p. 1007\)](#)
- [Condition keys for Identity And Access Management \(p. 1008\)](#)

Actions defined by Identity And Access 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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddClientIDToOpenIDConnectProvider	Grants permission to add a new client ID (audience) to the list of	Write	oidc-provider* (p. 1007)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	registered IDs for the specified IAM OpenID Connect (OIDC) provider resource				
AddRoleToInstanceProfile	Grants permission to add an IAM role to the specified instance profile	Write	instance-profile* (p. 1007)		iam:PassRole
AddUserToGroup	Grants permission to add an IAM user to the specified IAM group	Write	group* (p. 1007)		
AttachGroupPolicy	Grants permission to attach a managed policy to the specified IAM group	Permissions management	group* (p. 1007)		iam:PolicyARN (p. 1008)
AttachRolePolicy	Grants permission to attach a managed policy to the specified IAM role	Permissions management	role* (p. 1007)		iam:PolicyARN (p. 1008) iam:PermissionsBoundary (p. 1008)
AttachUserPolicy	Grants permission to attach a managed policy to the specified IAM user	Permissions management	user* (p. 1008)		iam:PolicyARN (p. 1008) iam:PermissionsBoundary (p. 1008)
ChangePassword	Grants permission for an IAM user to change their own password	Write	user* (p. 1008)		
CreateAccessKey	Grants permission to create access key and secret access key for the specified IAM user	Write	user* (p. 1008)		
CreateAccountAlias	Grants permission to create an alias for your AWS account	Write			
CreateGroup	Grants permission to create a new group	Write	group* (p. 1007)		
CreateInstanceProfile	Grants permission to create a new instance profile	Write	instance-profile* (p. 1007)		aws:TagKeys (p. 1008) aws:RequestTag/\${TagKey} (p. 1008)
CreateLoginProfile	Grants permission to create a password for the specified IAM user	Write	user* (p. 1008)		

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* (p. 1007)		
				aws:TagKeys (p. 1008)	aws:RequestTag/\${TagKey} (p. 1008)
CreatePolicy	Grants permission to create a new managed policy	Permissions management	policy* (p. 1007)	aws:TagKeys (p. 1008)	aws:RequestTag/\${TagKey} (p. 1008)
CreatePolicyVersion	Grants permission to create a new version of the specified managed policy	Permissions management	policy* (p. 1007)		
CreateRole	Grants permission to create a new role	Write	role* (p. 1007)		iam:PermissionsBoundary (p. 1008)
	aws:TagKeys (p. 1008)		aws:RequestTag/\${TagKey} (p. 1008)		
CreateSAMLProvider	Grants permission to create an IAM resource that describes an identity provider (IdP) that supports SAML 2.0	Write	saml-provider* (p. 1007)		
	aws:TagKeys (p. 1008)	aws:RequestTag/\${TagKey} (p. 1008)			
CreateServiceLinkedRole	Grants permission to create an IAM role that allows an AWS service to perform actions on your behalf	Write	role* (p. 1007)		iam:AWSServiceName (p. 1008)
CreateServiceSpecificCredential	Grants permission to create a new service-specific credential for an IAM user	Write	user* (p. 1008)		
CreateUser	Grants permission to create a new IAM user	Write	user* (p. 1008)		
	iam:PermissionsBoundary (p. 1008)		aws:TagKeys (p. 1008) aws:RequestTag/\${TagKey} (p. 1008)		
CreateVirtualMFADevice	Grants permission to create a new virtual MFA device	Write	mfa* (p. 1007)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys (p. 1008) aws:RequestTag/ \${TagKey} (p. 1008)	
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* (p. 1008)		
DeleteAccessKey	Grants permission to delete the access key pair that is associated with the specified IAM user	Write	user* (p. 1008)		
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			
DeleteGroup	Grants permission to delete the specified IAM group	Write	group* (p. 1007)		
DeleteGroupPolicy	Grants permission to delete the specified inline policy from its group	Permissions management	group* (p. 1007)		
DeleteInstanceProfile	Grants permission to delete the specified instance profile	Write	instance-profile* (p. 1007)		
DeleteLoginProfile	Grants permission to delete the password for the specified IAM user	Write	user* (p. 1008)		
DeleteOpenIDConnectProvider	Grants permission to delete an OpenID Connect identity provider (IdP) resource object in IAM	Write	oidc-provider* (p. 1007)		
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* (p. 1007)		
DeletePolicyVersion	Grants permission to delete a version from the specified managed policy	Permissions management	policy* (p. 1007)		
DeleteRole	Grants permission to delete the specified role	Write	role* (p. 1007)		
DeleteRolePermissionsBoundary		Permissions management	role* (p. 1007)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to remove the permissions boundary from a role			iam:PermissionsBoundary (p. 1008)	
DeleteRolePolicy	Grants permission to delete the specified inline policy from the specified role	Permissions management	role* (p. 1007)	iam:PermissionsBoundary (p. 1008)	
DeleteSAMLProvider	Grants permission to delete a SAML provider resource in IAM	Write	saml-provider* (p. 1007)		
DeleteSSHPublicKey	Grants permission to delete the specified SSH public key	Write	user* (p. 1008)		
DeleteServerCertificate	Grants permission to delete the specified server certificate	Write	server-certificate* (p. 1007)		
DeleteServiceLink	Grants permission to delete the IAM role that is linked to a specific AWS service, if the service is no longer using it	Write	role* (p. 1007)		
DeleteServiceSpecificCredential	Grants permission to delete the specified service-specific credential for an IAM user	Write	user* (p. 1008)		
DeleteSigningCertificate	Grants permission to delete the signing certificate that is associated with the specified IAM user	Write	user* (p. 1008)		
DeleteUser	Grants permission to delete the specified IAM user	Write	user* (p. 1008)		
DeleteUserPermissionsBoundary	Grants permission to remove the permissions boundary from the specified IAM user	Permissions management	user* (p. 1008)	iam:PermissionsBoundary (p. 1008)	
DeleteUserPolicy	Grants permission to delete the specified inline policy from an IAM user	Permissions management	user* (p. 1008)	iam:PermissionsBoundary (p. 1008)	
DeleteVirtualMFADevice	Grants permission to delete a virtual MFA device	Write	mfa (p. 1007)		
			sms-mfa (p. 1008)		
DetachGroupPolicy	Grants permission to detach a managed policy from the specified IAM group	Permissions management	group* (p. 1007)	iam:PolicyARN (p. 1008)	
DetachRolePolicy	Grants permission to detach a managed policy from the specified role	Permissions management	role* (p. 1007)	iam:PolicyARN (p. 1008)	iam:PermissionsBoundary (p. 1008)

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* (p. 1008)	iam:PolicyARN (p. 1008)	iam:PermissionsBoundary (p. 1008)	
EnableMFADevice	Grants permission to enable an MFA device and associate it with the specified IAM user	Write	user* (p. 1008)			
GenerateCredentialReport	Grants permission to generate a credential report for the AWS account	Read				
GenerateOrganizationAccessReport	Grants permission to generate an access report for an AWS Organizations entity	Read	access-report* (p. 1007)		organizations:DescribePolicy organizations>ListChildren organizations>ListParents organizations>ListPolicies organizations>ListRoots organizations>ListTargets	
					iam:OrganizationsPolicyId (p. 1008)	
GenerateServiceLastAccessed	Grants permission to generate a service last accessed data report for an IAM resource	Read	group* (p. 1007)			
				policy* (p. 1007)		
				role* (p. 1007)		
				user* (p. 1008)		
GetAccessKeyLastUsed	Grants permission to retrieve information about when the specified access key was last used	Read	user* (p. 1008)			
GetAccountAuthorizationInformation	Grants permission to retrieve information about all IAM users, groups, roles, and policies in your AWS account, including their relationships to one another	Read				
GetAccountPasswordPolicy	Grants permission to retrieve the password policy for the AWS account	Read				
GetAccountSummary	Grants permission to retrieve information about IAM entity usage and IAM quotas in the AWS account	List				

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetContextKeysForPolicy	Grants permission to retrieve a list of all the context keys that are referenced in the specified policy	Read			
GetContextKeysForUser	Grants permission to retrieve a list of all the context keys that are referenced in all IAM policies that are attached to the specified IAM identity (user, group, or role)	Read	group (p. 1007)		
			role (p. 1007)		
			user (p. 1008)		
GetCredentialReport	Grants permission to retrieve a credential report for the AWS account	Read			
GetGroup	Grants permission to retrieve a list of IAM users in the specified IAM group	Read	group* (p. 1007)		
GetGroupPolicy	Grants permission to retrieve an inline policy document that is embedded in the specified IAM group	Read	group* (p. 1007)		
GetInstanceProfile	Grants permission to retrieve information about the specified instance profile, including the instance profile's path, GUID, ARN, and role	Read	instance-profile* (p. 1007)		
GetLoginProfile	Grants permission to retrieve the user name and password creation date for the specified IAM user	List	user* (p. 1008)		
GetOpenIDConnectProvider	Grants permission to retrieve information about the specified OpenID Connect (OIDC) provider resource in IAM	Read	oidc-provider* (p. 1007)		
GetOrganizationsAWSOrganizations	Grants permission to retrieve an AWS Organizations access report	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* (p. 1007)		
GetPolicyVersion	Grants permission to retrieve information about a version of the specified managed policy, including the policy document	Read	policy* (p. 1007)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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* (p. 1007)		
GetRolePolicy	Grants permission to retrieve an inline policy document that is embedded with the specified IAM role	Read	role* (p. 1007)		
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* (p. 1007)		
GetSSHPublicKey	Grants permission to retrieve the specified SSH public key, including metadata about the key	Read	user* (p. 1008)		
GetServerCertificate	Grants permission to retrieve information about the specified server certificate stored in IAM	Read	server-certificate* (p. 1007)		
GetServiceLastAccessedData	Grants permission to retrieve information about the service last accessed data report	Read			
GetServiceLastAccessedDataWithEntities	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* (p. 1007)		
 GetUser	Grants permission to retrieve information about the specified IAM user, including the user's creation date, path, unique ID, and ARN	Read	user* (p. 1008)		
 GetUserPolicy	Grants permission to retrieve an inline policy document that is embedded in the specified IAM user	Read	user* (p. 1008)		
 ListAccessKeys	Grants permission to list information about the access key IDs that are associated with the specified IAM user	List	user* (p. 1008)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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* (p. 1007)		
ListAttachedRolePolicies	Grants permission to list all managed policies that are attached to the specified IAM role	List	role* (p. 1007)		
ListAttachedUserPolicies	Grants permission to list all managed policies that are attached to the specified IAM user	List	user* (p. 1008)		
ListEntitiesForPolicy	Grants permission to list all IAM identities to which the specified managed policy is attached	List	policy* (p. 1007)		
ListGroupPolicies	Grants permission to list the names of the inline policies that are embedded in the specified IAM group	List	group* (p. 1007)		
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* (p. 1008)		
ListInstanceProfileTags	Grants permission to list the tags that are attached to the specified instance profile	List	instance-profile* (p. 1007)		
ListInstanceProfiles	Grants permission to list the instance profiles that have the specified path prefix	List	instance-profile* (p. 1007)		
ListInstanceProfileRoles	Grants permission to list the instance profiles that have the specified associated IAM role	List	role* (p. 1007)		
ListMFADeviceTags	Grants permission to list the tags that are attached to the specified virtual mfa device	List	mfa* (p. 1007)		
ListMFADevices	Grants permission to list the MFA devices for an IAM user	List	user (p. 1008)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListOpenIDConnectTags	Grants permission to list the tags that are attached to the specified OpenID Connect provider	List	oidc-provider* (p. 1007)		
ListOpenIDConnectInformation	Grants permission to list information about the IAM OpenID Connect (OIDC) provider resource objects that are defined in the AWS account	List			
ListPolicies	Grants permission to list all managed policies	List			
ListPoliciesGrantingInformation	Grants permission to list information about the policies that grant an entity access to a specific service	List	group* (p. 1007)		
			role* (p. 1007)		
			user* (p. 1008)		
ListPolicyTags	Grants permission to list the tags that are attached to the specified managed policy	List	policy* (p. 1007)		
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* (p. 1007)		
ListRolePolicies	Grants permission to list the names of the inline policies that are embedded in the specified IAM role	List	role* (p. 1007)		
ListRoleTags	Grants permission to list the tags that are attached to the specified IAM role	List	role* (p. 1007)		
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* (p. 1007)		
ListSAMLProviderInformation	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* (p. 1008)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListServerCertificates	Grants permission to list the tags that are attached to the specified server certificate	List	server-certificate* (p. 1007)		
ListServerCertificateSignatures	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* (p. 1008)		
ListSigningCertificates	Grants permission to list information about the signing certificates that are associated with the specified IAM user	List	user* (p. 1008)		
ListUserPolicies	Grants permission to list the names of the inline policies that are embedded in the specified IAM user	List	user* (p. 1008)		
ListUserTags	Grants permission to list the tags that are attached to the specified IAM user	List	user* (p. 1008)		
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* (p. 1007)		
				iam:AssociatedResourceArn (p. 1008)	
				iam:PassedToService (p. 1008)	
PutGroupPolicy	Grants permission to create or update an inline policy document that is embedded in the specified IAM group	Permissions management	group* (p. 1007)		
PutRolePermissionsBoundary	Grants permission to set a managed policy as a permissions boundary for a role			role* (p. 1007)	
PutRolePolicy	Grants permission to create or update an inline policy document that is embedded in the specified IAM role			iam:PermissionsBoundary (p. 1008)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutUserPermissionsBoundary	Grants permission to set a managed policy as a permissions boundary for an IAM user	Permissions management	user* (p. 1008)		
PutUserPolicy	Grants permission to create or update an inline policy document that is embedded in the specified IAM user	Permissions management	user* (p. 1008)		iam:PermissionsBoundary (p. 1008)
RemoveClientIDFromOpenIDProvider	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* (p. 1007)		
RemoveRoleFromInstanceProfile	Grants permission to remove an IAM role from the specified EC2 instance profile	Write	instance-profile* (p. 1007)		
RemoveUserFromGroup	Grants permission to remove a IAM user from the specified group	Write	group* (p. 1007)		
ResetServiceSpecificPassword	Grants permission to reset the password for an existing service-specific credential for an IAM user	Write	user* (p. 1008)		
ResyncMFADevice	Grants permission to synchronize the specified MFA device with its IAM entity (user or role)	Write	user* (p. 1008)		
SetDefaultPolicyVersion	Grants permission to set the version of the specified policy as the policy's default version	Permissions management	policy* (p. 1007)		
SetSecurityTokenGlobalEndpoint	Grants permission to set the STS 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 (p. 1007)		
			role (p. 1007)		
			user (p. 1008)		
TagInstanceProfile	Grants permission to add tags to an instance profile	Tagging	instance-profile* (p. 1007)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys (p. 1008) aws:RequestTag/ {\$TagKey} (p. 1008)	
TagMFADevice	Grants permission to add tags to a virtual mfa device	Tagging	mfa* (p. 1007)		
				aws:TagKeys (p. 1008) aws:RequestTag/ {\$TagKey} (p. 1008)	
TagOpenIDConnectProvider	Grants permission to add tags to an OpenID Connect provider	Tagging	oidc-provider* (p. 1007)		
				aws:TagKeys (p. 1008) aws:RequestTag/ {\$TagKey} (p. 1008)	
TagPolicy	Grants permission to add tags to a managed policy	Tagging	policy* (p. 1007)		
				aws:TagKeys (p. 1008) aws:RequestTag/ {\$TagKey} (p. 1008)	
TagRole	Grants permission to add tags to an IAM role	Tagging	role* (p. 1007)		
				aws:TagKeys (p. 1008) aws:RequestTag/ {\$TagKey} (p. 1008)	
TagSAMLProvider	Grants permission to add tags to a SAML Provider	Tagging	saml-provider* (p. 1007)		
				aws:TagKeys (p. 1008) aws:RequestTag/ {\$TagKey} (p. 1008)	
TagServerCertificate	Grants permission to add tags to a server certificate	Tagging	server-certificate* (p. 1007)		
				aws:TagKeys (p. 1008) aws:RequestTag/ {\$TagKey} (p. 1008)	
TagUser	Grants permission to add tags to an IAM user	Tagging	user* (p. 1008)		
				aws:TagKeys (p. 1008) aws:RequestTag/ {\$TagKey} (p. 1008)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagInstanceProfile	Grants permission to remove the specified tags from the instance profile	Tagging	instance-profile* (p. 1007)		
			aws:TagKeys (p. 1008)		
UntagMFADevice	Grants permission to remove the specified tags from the virtual mfa device	Tagging	mfa* (p. 1007)		
			aws:TagKeys (p. 1008)		
UntagOpenIDConnect	Grants permission to remove the specified tags from the OpenID Connect provider	Tagging	oidc-provider* (p. 1007)		
			aws:TagKeys (p. 1008)		
UntagPolicy	Grants permission to remove the specified tags from the managed policy	Tagging	policy* (p. 1007)		
			aws:TagKeys (p. 1008)		
UntagRole	Grants permission to remove the specified tags from the role	Tagging	role* (p. 1007)		
			aws:TagKeys (p. 1008)		
UntagSAMLProvider	Grants permission to remove the specified tags from the SAML Provider	Tagging	saml-provider* (p. 1007)		
			aws:TagKeys (p. 1008)		
UntagServerCertificate	Grants permission to remove the specified tags from the server certificate	Tagging	server-certificate* (p. 1007)		
			aws:TagKeys (p. 1008)		
UntagUser	Grants permission to remove the specified tags from the user	Tagging	user* (p. 1008)		
			aws:TagKeys (p. 1008)		
UpdateAccessKey	Grants permission to update the status of the specified access key as Active or Inactive	Write	user* (p. 1008)		
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* (p. 1007)		
UpdateGroup	Grants permission to update the name or path of the specified IAM group	Write	group* (p. 1007)		
UpdateLoginProfile	Grants permission to change the password for the specified IAM user	Write	user* (p. 1008)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateOpenIDConnectProviderList	Grants permission to update the thumbprints that are associated with an OpenID Connect (OIDC) provider resource	Write	oidc-provider* (p. 1007)		
UpdateRole	Grants permission to update the description or maximum session duration setting of a role	Write	role* (p. 1007)		
UpdateRoleDescription	Grants permission to update the description of a role	Write	role* (p. 1007)		
UpdateSAMLProviderMetadata	Grants permission to update the metadata document for an existing SAML provider resource	Write	saml-provider* (p. 1007)		
UpdateSSHPublicKey	Grants permission to update the status of an IAM user's SSH public key to active or inactive	Write	user* (p. 1008)		
UpdateServerCertificate	Grants permission to update the name or the path of the specified server certificate stored in IAM	Write	server-certificate* (p. 1007)		
UpdateServiceSpecificCredential	Grants permission to update the status of a service-specific credential to active or inactive for an IAM user	Write	user* (p. 1008)		
UpdateSigningCert	Grants permission to update the status of the specified user signing certificate to active or disabled	Write	user* (p. 1008)		
UpdateUser	Grants permission to update the name or the path of the specified IAM user	Write	user* (p. 1008)		
UploadSSHPublicKey	Grants permission to upload an SSH public key and associate it with the specified IAM user	Write	user* (p. 1008)		
UploadServerCertificate	Grants permission to upload a server certificate entity for the AWS account	Write	server-certificate* (p. 1007)		
			aws:TagKeys (p. 1008) aws:RequestTag/\${TagKey} (p. 1008)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UploadSigningCert	Grants permission to upload an X.509 signing certificate and associate it with the specified IAM user	Write	user* (p. 1008)		

Resource types defined by Identity And Access 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 \(p. 992\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
access-report	arn:\${Partition}:iam:::\${Account}:access-report/\${EntityPath}	
assumed-role	arn:\${Partition}:iam:::\${Account}:assumed-role/\${RoleName}/\${RoleSessionName}	
federated-user	arn:\${Partition}:iam:::\${Account}:federated-user/\${UserName}	
group	arn:\${Partition}:iam:::\${Account}:group/\${GroupNameWithPath}	
instance-profile	arn:\${Partition}:iam:::\${Account}:instance-profile/\${InstanceProfileNameWithPath}	aws:ResourceTag/\${TagKey} (p. 1008)
mfa	arn:\${Partition}:iam:::\${Account}:mfa/\${MfaTokenIdWithPath}	aws:ResourceTag/\${TagKey} (p. 1008)
oidc-provider	arn:\${Partition}:iam:::\${Account}:oidc-provider/\${OidcProviderName}	aws:ResourceTag/\${TagKey} (p. 1008)
policy	arn:\${Partition}:iam:::\${Account}:policy/\${PolicyNameWithPath}	aws:ResourceTag/\${TagKey} (p. 1008)
role	arn:\${Partition}:iam:::\${Account}:role/\${RoleNameWithPath}	aws:ResourceTag/\${TagKey} (p. 1008) iam:ResourceTag/\${TagKey} (p. 1008)
saml-provider	arn:\${Partition}:iam:::\${Account}:saml-provider/\${SamlProviderName}	aws:ResourceTag/\${TagKey} (p. 1008)
server-certificate	arn:\${Partition}:iam:::\${Account}:server-certificate/\${CertificateNameWithPath}	aws:ResourceTag/\${TagKey} (p. 1008)

Resource types	ARN	Condition keys
sms-mfa	arn:\${Partition}:iam::\${Account}:sms-mfa/\${MfaTokenIdWithPath}	
user	arn:\${Partition}:iam::\${Account}:user/\${UserNameWithPath}	aws:ResourceTag/\${TagKey} (p. 1008) iam:ResourceTag/\${TagKey} (p. 1008)

Condition keys for Identity And Access Management

Identity And Access 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 [Available global condition 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:AWSServiceNameAttached	Filters access by the AWS service to which this role is attached	String
iam:AssociatedResourceArn	Filters by the resource that the role will be used on behalf of	ARN
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)	String
iam:PolicyARN	Filters access by the ARN of an IAM policy	ARN
iam:ResourceTag/\${TagKey}	Filters access by the tags attached to an IAM entity (user or role)	String

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 \(p. 1009\)](#)
- [Resource types defined by AWS Identity Store \(p. 1010\)](#)
- [Condition keys for AWS Identity Store \(p. 1010\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeGroup	Grants permission to retrieves information about group from the directory that AWS Identity Store provides by default	Read			
DescribeUser	Grants permission to retrieves information about user from the directory that AWS Identity Store provides by default	Read			
ListGroups	Grants permission to search for groups within the associated directory	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListUsers	Grants permission to search for users within the associated directory	List			

Resource types defined by AWS Identity Store

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

Condition keys for AWS Identity Store

Identity Store 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 [Available keys for conditions](#).

Actions, resources, and condition keys for AWS Identity Synchronization Service

AWS Identity Synchronization Service (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 Synchronization Service \(p. 1010\)](#)
- [Resource types defined by AWS Identity Synchronization Service \(p. 1011\)](#)
- [Condition keys for AWS Identity Synchronization Service \(p. 1012\)](#)

Actions defined by AWS Identity Synchronization 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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("**") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSyncFilter	Grants permission to create a sync filter on the sync profile	Write	SyncProfileResource* (p. 1012)		
CreateSyncProfile	Grants permission to create a sync profile for the source	Write			ds:AuthorizeApplication
CreateSyncTarget	Grants permission to create a sync target for the source	Write	SyncProfileResource* (p. 1012)		
DeleteSyncFilter	Grants permission to delete a sync filter on the sync profile	Write	SyncProfileResource* (p. 1012)		
DeleteSyncProfile	Grants permission to delete a sync profile on the source	Write	SyncProfileResource* (p. 1012)		ds:UnauthorizeApplication
DeleteSyncTarget	Grants permission to delete a sync target on the source	Write	SyncProfileResource* (p. 1012) SyncTargetResource* (p. 1012)		
GetSyncProfile	Grants permission to retrieve a sync profile using sync profile name	Read	SyncProfileResource* (p. 1012)		
GetSyncTarget	Grants permission to retrieve a sync target on the sync profile	Read	SyncProfileResource* (p. 1012) SyncTargetResource* (p. 1012)		
ListSyncFilters	Grants permission to list the sync filters on the sync profile	List	SyncProfileResource* (p. 1012)		
StartSync	Grants permission to start a synchronization process or to restart a synchronization that was previously stopped	Write	SyncProfileResource* (p. 1012)		
StopSync	Grants permission to stop any planned synchronizations in the synchronization schedule from starting	Write	SyncProfileResource* (p. 1012)		
UpdateSyncTarget	Grants permission to update a sync target on the sync profile	Write	SyncProfileResource* (p. 1012) SyncTargetResource* (p. 1012)		

Resource types defined by AWS Identity Synchronization 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](#) (p. 1010) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
SyncProfileResource	<code>^arn:\${Partition}:identity-sync:\${Region}: \${Account}:profile/\${SyncProfileName}</code>	
SyncTargetResource	<code>^arn:\${Partition}:identity-sync:\${Region}: \${Account}:target/\${SyncProfileName}/ \${SyncTargetName}</code>	

Condition keys for AWS Identity Synchronization Service

IdentitySync 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 [Available keys for conditions](#).

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 \(p. 1012\)](#)
- [Resource types defined by AWS Import Export Disk Service \(p. 1013\)](#)
- [Condition keys for AWS Import Export Disk Service \(p. 1013\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 signature value associated with the job.	Read			
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 [Available keys for conditions](#).

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 \(p. 1014\)](#)
- [Resource types defined by Amazon Inspector \(p. 1018\)](#)
- [Condition keys for Amazon Inspector \(p. 1018\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 <code>AddAttributes</code> (key and value pairs) to the findings that are specified by the ARNs of the findings	Write			
CreateAssessmentTargets	Grants permission to create <code>CreateAssessmentTarget</code> using the ARN of the resource group that is generated by <code>CreateResourceGroup</code>	Write			
CreateAssessmentTemplates	Grants permission to create <code>CreateAssessmentTemplate</code> for the assessment target that is specified by the ARN of the assessment target	Write			
CreateExclusionsPreview	Grants permission to start the <code>CreateExclusionsPreview</code> of an exclusions preview for the specified assessment template	Write			
CreateResourceGroups	Grants permission to create <code>CreateResourceGroup</code> using the specified set of tags (key and	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	value pairs) that are used to select the EC2 instances to be included in an Amazon Inspector assessment target				
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			
DescribeAssessmentTemplates	Grants permission to describe the assessment templates that are specified by the ARNs of the assessment templates	Read			
DescribeCrossAccountAccess	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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeRulesPackages	Grants permission to describe the rules packages that are specified by the ARNs of the rules packages	Read			
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			
GetTelemetryMetrics	Grants permission to get information about the data that is collected for the specified assessment run	Read			
ListAssessmentRuns	Grants permission to list the agents of the assessment runs that are specified by the ARNs of the assessment runs	List			
ListAssessmentRunTemplates	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			
ListAssessmentTemplateAssessments	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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
PreviewAgents	Grants permission to preview the agents installed on the EC2 instances that are part of the specified assessment target	Read			
RegisterCrossAccountAgents	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			
StopAssessmentRun	Grants permission to stop the assessment run that is specified by the ARN of the assessment run	Write			
SubscribeToEvents	Grants permission to enable the process of sending Amazon Simple Notification Service (SNS) notifications about a specified event to a specified SNS topic	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UnsubscribeFromTopic	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 [Available keys for conditions](#).

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 \(p. 1018\)](#)
- [Resource types defined by Amazon Inspector2 \(p. 1021\)](#)
- [Condition keys for Amazon Inspector2 \(p. 1022\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateMember	Grants permission to associate an account with an Amazon Inspector administrator account	Write			
BatchGetAccountInformation	Grants permission to retrieve information about Amazon Inspector accounts for an account	Read			
BatchGetFreeTrialEligibility	Grants permission to retrieve free trial period eligibility about Amazon Inspector accounts for an account	Read			
CancelFindingsReport	Grants permission to cancel the generation of a findings report	Write			
CreateFilter	Grants permission to create and define the settings for a findings filter	Write	Filter* (p. 1022)		
				aws:RequestTag/\${TagKey} (p. 1022)	
				aws:TagKeys (p. 1022)	
CreateFindingsReport	Grants permission to request the generation of a findings report	Write			
DeleteFilter	Grants permission to delete a findings filter	Write	Filter* (p. 1022)		
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			
DisableDelegatedAdministrator	Grants permission to disable an account as the delegated Amazon Inspector administrator account for an AWS organization	Write			
DisassociateMember	Grants permission to disassociate an Amazon Inspector administrator	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	account to disassociate from an Inspector member account				
Enable	Grants permission to enable and specify the configuration settings for a new Amazon Inspector account	Write			
EnableDelegatedAdministrator	Grants permission to enable an account as the delegated Amazon Inspector administrator account for an AWS organization	Write			
GetDelegatedAdministrator	Grants permission to retrieve information about the Amazon Inspector administrator account for an account	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			
ListAccountPermissions	Grants permission to retrieve feature configuration permissions associated with an Amazon Inspector account within an organization	List			
ListCoverage	Grants permission to retrieve the types of statistics Amazon Inspector can generate for resources Inspector monitors	List			
ListCoverageStatistics	Grants permission to retrieve statistical data and other information about the resources Amazon Inspector monitors	List			
ListDelegatedAdministrator	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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListFindingAggregates	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			
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			
TagResource	Grants permission to add or update the tags for an Amazon Inspector resource	Tagging		aws:RequestTag/\${TagKey} (p. 1022) aws:TagKeys (p. 1022) aws:ResourceTag/\${TagKey} (p. 1022)	
UntagResource	Grants permission to remove tags from an Amazon Inspector resource	Tagging		aws:TagKeys (p. 1022)	
UpdateFilter	Grants permission to update the settings for a findings filter	Write	Filter* (p. 1022)		
UpdateOrganization	Grants permission to update Amazon Inspector configuration settings for an AWS organization		aws:RequestTag/\${TagKey} (p. 1022) aws:TagKeys (p. 1022)		

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 \(p. 1018\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1022)
Finding	arn:\${Partition}:inspector2:\${Region}: \${Account}:finding/\${FindingId}	

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 [Available global condition 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 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 \(p. 1022\)](#)
- [Resource types defined by Amazon Interactive Video Service \(p. 1026\)](#)
- [Condition keys for Amazon Interactive Video Service \(p. 1026\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1026)		
BatchGetStreamKey	Grants permission to get multiple stream keys simultaneously by stream key ARN	Read	Stream-Key* (p. 1026)		
CreateChannel	Grants permission to create a new channel and an associated stream key	Write	Channel* (p. 1026)		
			Stream-Key* (p. 1026)		
				aws:TagKeys (p. 1027) aws:RequestTag/\${TagKey} (p. 1027)	
CreateRecording	Grants permission to create a new recording configuration	Write	Recording-Configuration* (p. 1026)		
				aws:TagKeys (p. 1027) aws:RequestTag/\${TagKey} (p. 1027)	
CreateStreamKey	Grants permission to create a stream key	Write	Stream-Key* (p. 1026)		
				aws:TagKeys (p. 1027) aws:RequestTag/\${TagKey} (p. 1027)	
DeleteChannel	Grants permission to delete a channel and channel's stream keys	Write	Channel* (p. 1026)		
			Stream-Key* (p. 1026)		
DeletePlaybackKey	Grants permission to delete the playback key pair for a specified ARN	Write	Playback-Key-Pair* (p. 1026)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteRecordingConfiguration	Grants permission to delete a recording configuration for the specified ARN	Write	Recording-Configuration* (p. 1026)		
DeleteStreamKey	Grants permission to delete the stream key for a specified ARN	Write	Stream-Key* (p. 1026)		
GetChannel	Grants permission to get the channel configuration for a specified channel ARN	Read	Channel* (p. 1026)		
GetPlaybackKeyPair	Grants permission to get the playback keypair information for a specified ARN	Read	Playback-Key-Pair* (p. 1026)		
GetRecordingConfiguration	Grants permission to get the recording configuration for the specified ARN	Read	Recording-Configuration* (p. 1026)		
GetStream	Grants permission to get information about the active (live) stream on a specified channel	Read	Channel* (p. 1026)		
GetStreamKey	Grants permission to get stream-key information for a specified ARN	Read	Stream-Key* (p. 1026)		
GetStreamSession	Grants permission to get information about the stream session on a specified channel	Read	Channel* (p. 1026)		
ImportPlaybackKeyPair	Grants permission to import the public key	Write	Playback-Key-Pair* (p. 1026)		
				aws:TagKeys (p. 1027)	
				aws:RequestTag/\${TagKey} (p. 1027)	
ListChannels	Grants permission to get summary information about channels	List	Channel* (p. 1026)		
ListPlaybackKeyPairs	Grants permission to get summary information about playback key pairs	List	Playback-Key-Pair* (p. 1026)		
ListRecordingConfigurations	Grants permission to get summary information about recording configurations	List	Recording-Configuration* (p. 1026)		
ListStreamKeys	Grants permission to get summary information about stream keys	List	Channel* (p. 1026)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Stream-Key* (p. 1026)		
ListStreamSessions	Grants permission to get summary information about streams sessions on a specified channel	List	Channel* (p. 1026)		
ListStreams	Grants permission to get summary information about live streams	List	Channel* (p. 1026)		
ListTagsForResource	Grants permission to get information about the tags for a specified ARN	Read	Channel (p. 1026) Playback-Key-Pair (p. 1026) Recording-Configuration (p. 1026) Stream-Key (p. 1026)		
			aws:TagKeys (p. 1027) aws:RequestTag/\${TagKey} (p. 1027)		
PutMetadata	Grants permission to insert metadata into an RTMP stream for a specified channel	Write	Channel* (p. 1026)		
StopStream	Grants permission to disconnect a streamer on a specified channel	Write	Channel* (p. 1026)		
TagResource	Grants permission to add or update tags for a resource with a specified ARN	Tagging	Channel (p. 1026) Playback-Key-Pair (p. 1026) Recording-Configuration (p. 1026) Stream-Key (p. 1026)		
			aws:TagKeys (p. 1027) aws:RequestTag/\${TagKey} (p. 1027)		
UntagResource	Grants permission to remove tags for a resource with a specified ARN	Tagging	Channel (p. 1026)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Playback-Key-Pair (p. 1026)		
			Recording-Configuration (p. 1026)		
			Stream-Key (p. 1026)		
				aws:TagKeys (p. 1027)	
UpdateChannel	Grants permission to update a channel's configuration	Write	Channel* (p. 1026)		

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 \(p. 1022\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
Channel	<code>arn:\${Partition}:ivs:\${Region}: \${Account}:channel/\${ResourceId}</code>	aws:ResourceTag/ \${TagKey} (p. 1027)
Stream-Key	<code>arn:\${Partition}:ivs:\${Region}: \${Account}:stream-key/\${ResourceId}</code>	aws:ResourceTag/ \${TagKey} (p. 1027)
Playback-Key-Pair	<code>arn:\${Partition}:ivs:\${Region}: \${Account}:playback-key/\${ResourceId}</code>	aws:ResourceTag/ \${TagKey} (p. 1027)
Recording-Configuration	<code>arn:\${Partition}:ivs:\${Region}: \${Account}:recording-configuration/ \${ResourceId}</code>	aws:ResourceTag/ \${TagKey} (p. 1027)

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 [Available global condition 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	String

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 \(p. 1027\)](#)
- [Resource types defined by Amazon Interactive Video Service Chat \(p. 1029\)](#)
- [Condition keys for Amazon Interactive Video Service Chat \(p. 1029\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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	Write	Room* (p. 1029)		aws:TagKeys (p. 1029)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	WebSocket connection to a room			aws:RequestTag/\${TagKey} (p. 1029)	
CreateRoom	Grants permission to create a room that allows clients to connect and pass messages	Write	Room* (p. 1029)		
				aws:TagKeys (p. 1029) aws:RequestTag/\${TagKey} (p. 1029)	
DeleteMessage	Grants permission to send an event to a specific room which directs clients to delete a specific message	Write	Room* (p. 1029)		
DeleteRoom	Grants permission to delete the room for a specified room ARN	Write	Room* (p. 1029)		
DisconnectUser	Grants permission to disconnect all connections using a specified user ID from a room	Write	Room* (p. 1029)		
GetRoom	Grants permission to get the room configuration for a specified room ARN	Read	Room* (p. 1029)		
ListRooms	Grants permission to get summary information about rooms	List	Room* (p. 1029)		
ListTagsForResource	Grants permission to get information about the tags for a specified ARN	Read	Room (p. 1029)		
				aws:TagKeys (p. 1029) aws:RequestTag/\${TagKey} (p. 1029)	
SendEvent	Grants permission to send an event to a room	Write	Room* (p. 1029)		
TagResource	Grants permission to add or update tags for a resource with a specified ARN	Tagging	Room (p. 1029)		
				aws:TagKeys (p. 1029) aws:RequestTag/\${TagKey} (p. 1029)	
UntagResource	Grants permission to remove tags for a resource with a specified ARN	Tagging	Room (p. 1029)		
				aws:TagKeys (p. 1029)	
UpdateRoom	Grants permission to update the room configuration for a specified room ARN	Write	Room* (p. 1029)		

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 \(p. 1027\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
Room	<code>arn:\${Partition}:ivschat::\${Account}:room/\${ResourceId}</code>	aws:ResourceTag/\${TagKey} (p. 1029)

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters access by the tags associated with the request	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters access by the tags associated with the resource	String
<code>aws:TagKeys</code>	Filters access by the tag keys that are passed 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 \(p. 1030\)](#)
- [Resource types defined by AWS IoT \(p. 1051\)](#)
- [Condition keys for AWS IoT \(p. 1052\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1052)		
AddThingToBillingGroup	Grants permission to add a thing to the specified billing group	Write	billinggroup* (p. 1051)		
			thing* (p. 1051)		
AddThingToThingGroup	Grants permission to add a thing to the specified thing group	Write	thing* (p. 1051)		
			thinggroup* (p. 1051)		
AssociateTargetsWithJob	Grants permission to associate a group with a continuous job	Write	job* (p. 1051)		
			thing* (p. 1051)		
			thinggroup* (p. 1051)		
AttachPolicy	Grants permission to attach a policy to the specified target	Permissions management	cert (p. 1052) thinggroup (p. 1051)		
AttachPrincipalPolicy	Grants permission to attach the specified policy to the specified principal (certificate or other credential)	Permissions management	cert (p. 1052)		
AttachSecurityProfile	Grants permission to associate a Device Defender security profile with a thing group or with this account	Write	securityprofile* (p. 1052)		
			custommetric (p. 1052)		
			dimension (p. 1052)		
			thinggroup (p. 1051)		
AttachThingPrincipal	Grants permission to attach the specified principal to the specified thing	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelAuditMitigationAction	Grants permission to cancel a mitigation action 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 pending transfer for the specified certificate	Write	cert* (p. 1052)		
CancelDetectMitigationJob	Grants permission to cancel a Device Defender ML Detect mitigation action	Write			
CancelJob	Grants permission to cancel a job	Write	job* (p. 1051)		
CancelJobExecution	Grants permission to cancel a job execution on a particular device	Write	job* (p. 1051) thing* (p. 1051)		
ClearDefaultAuthenticator	Grants permission to clear the default authorizer	Write			
CloseTunnel	Grants permission to close a tunnel	Write	tunnel* (p. 1051)		
			iot:Delete (p. 1053)		
ConfirmTopicRuleDefinition	Grants permission to confirm a TopicRuleDestinationDestination	Write	destination* (p. 1052)		
Connect	Grants permission to connect as the specified client	Write	client* (p. 1051)		
CreateAuditSuppression	Grants permission to create a Device Defender audit suppression	Write			
CreateAuthorizer	Grants permission to create an authorizer	Write	authorizer* (p. 1051) aws:RequestTag/ {\$TagKey} (p. 1053)		
				aws:TagKeys (p. 1053)	
CreateBillingGroup	Grants permission to create a billing group	Write	billinggroup* (p. 1051) aws:RequestTag/ {\$TagKey} (p. 1053)		
				aws:TagKeys (p. 1053)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCertificateFromX509	Grants permission to create an X.509 certificate using the specified certificate signing request	Write			
CreateCustomMetric	Grants permission to create a custom metric for device side metric reporting and monitoring	Write	custommetric* (p. 1052)		
CreateDimension	Grants permission to define a dimension that can be used to limit the scope of a metric used in a security profile	Write	dimension* (p. 1052)		
CreateDomainConfiguration	Grants permission to create a domain configuration	Write	domainconfiguration* (p. 1052)		
CreateDynamicThingGroup	Grants permission to create a Dynamic Thing Group	Write	dynamicthinggroup* (p. 1051)		
CreateFleetMetric	Grants permission to create a fleet metric	Write	fleetmetric* (p. 1051)		
			index* (p. 1051)		
			aws:RequestTag/ \${TagKey} (p. 1053)		
			aws:TagKeys (p. 1053)		
CreateJob	Grants permission to create a job	Write	job* (p. 1051)		
			thing* (p. 1051)		
			thinggroup* (p. 1051)		
			jobtemplate (p. 1051)		
			aws:RequestTag/ \${TagKey} (p. 1053)		
			aws:TagKeys (p. 1053)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions	
CreateJobTemplate	Grants permission to create a job template	Write	jobtemplate* (p. 1051) job (p. 1051)			
			aws:RequestTag/ {\$TagKey} (p. 1053)			
			aws:TagKeys (p. 1053)			
CreateKeysAndCertificates	Grants permission to create a 2048-bit RSA key pair and issues an X.509 certificate using the issued public key	Write				
CreateMitigationAction	Grants permission to define an action that can be applied to audit findings by using StartAuditMitigationActionsTask	Write	mitigationaction* (p. 1052) aws:RequestTag/ {\$TagKey} (p. 1053)			
			aws:TagKeys (p. 1053)			
	otaupdate* (p. 1052) aws:RequestTag/ {\$TagKey} (p. 1053)					
CreateOTAUpdate		Grants permission to create an OTA update job	Write			
aws:TagKeys (p. 1053)						
CreatePolicy	Grants permission to create an AWS IoT policy	Write	policy* (p. 1051) aws:RequestTag/ {\$TagKey} (p. 1053)			
CreatePolicyVersion	Grants permission to create a new version of the specified AWS IoT policy		aws:RequestTag/ {\$TagKey} (p. 1053)			
CreateProvisioningClaim	Grants permission to create a provisioning claim	Write	provisioningtemplate* (p. 1052)			
CreateProvisioningTemplate	Grants permission to create a fleet provisioning template	Write	provisioningtemplate* (p. 1052) aws:RequestTag/ {\$TagKey} (p. 1053)	iam:PassRole		
			aws:RequestTag/ {\$TagKey} (p. 1053)			
			aws:TagKeys (p. 1053)			
CreateProvisioningTemplateVersion	Grants permission to create a new version of a fleet provisioning template	Write	provisioningtemplate* (p. 1052)			
CreateRoleAlias	Grants permission to create a role alias	Write	rolealias* (p. 1051)	iam:PassRole		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 1053) aws:TagKeys (p. 1053)	
CreateScheduledAudit	Grants permission to create a scheduled audit that is run at a specified time interval	Write	scheduledaudit* (p. 1052)		
				aws:RequestTag/ \${TagKey} (p. 1053) aws:TagKeys (p. 1053)	
CreateSecurityProfile	Grants permission to create a Device Defender security profile	Write	securityprofile* (p. 1052) custommetric (p. 1052) dimension (p. 1052)		
				aws:RequestTag/ \${TagKey} (p. 1053) aws:TagKeys (p. 1053)	
CreateStream	Grants permission to create a new AWS IoT stream	Write	stream* (p. 1052)		
				aws:RequestTag/ \${TagKey} (p. 1053) aws:TagKeys (p. 1053)	
CreateThing	Grants permission to create a thing in the thing registry	Write	thing* (p. 1051) billinggroup (p. 1051)		
				aws:RequestTag/ \${TagKey} (p. 1053) aws:TagKeys (p. 1053)	
CreateThingGroup	Grants permission to create a thing group	Write	thinggroup* (p. 1051)		
				aws:RequestTag/ \${TagKey} (p. 1053) aws:TagKeys (p. 1053)	
CreateThingType	Grants permission to create a new thing type	Write	thingtype* (p. 1051)		
				aws:RequestTag/ \${TagKey} (p. 1053) aws:TagKeys (p. 1053)	
CreateTopicRule	Grants permission to create a rule	Write	rule* (p. 1052)		
				aws:RequestTag/ \${TagKey} (p. 1053) aws:TagKeys (p. 1053)	
CreateTopicRuleDestination	Grants permission to create a Topic Rule Destination	Write	destination* (p. 1052)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAccountAuditConfiguration	Grants permission to delete the audit configuration associated with the account	Write			
DeleteAuditSuppression	Grants permission to delete Device Defender audit suppression	Write			
DeleteAuthorizer	Grants permission to delete the specified authorizer	Write	authorizer* (p. 1051)		
DeleteBillingGroup	Grants permission to delete the specified billing group	Write	billinggroup* (p. 1051)		
DeleteCACertificate	Grants permission to delete a registered CA certificate	Write	cacert* (p. 1052)		
DeleteCertificate	Grants permission to delete the specified certificate	Write	cert* (p. 1052)		
DeleteCustomMetric	Grants permission to delete the specified custom metric from your AWS account	Write	custommetric* (p. 1052)		
DeleteDimension	Grants permission to remove the specified dimension from your AWS account	Write	dimension* (p. 1052)		
DeleteDomainConfiguration	Grants permission to delete a domain configuration	Write	domainconfiguration* (p. 1052)		
DeleteDynamicThingGroup	Grants permission to delete the specified Dynamic Thing Group	Write	dynamicthinggroup* (p. 1051)		
DeleteFleetMetric	Grants permission to delete the specified fleet metric	Write	fleetmetric* (p. 1051)		
DeleteJob	Grants permission to delete a job and its related job executions	Write	job* (p. 1051)		
DeleteJobExecution	Grants permission to delete a job execution	Write	job* (p. 1051) thing* (p. 1051)		
DeleteJobTemplate	Grants permission to delete a job template	Write	jobtemplate* (p. 1051)		
DeleteMitigationAction	Grants permission to delete a defined mitigation action from your AWS account	Write	mitigationaction* (p. 1052)		
DeleteOTAUpdate	Grants permission to delete an OTA update job	Write	otaupdate* (p. 1052)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeletePolicy	Grants permission to delete the specified policy	Write	policy* (p. 1051)		
DeletePolicyVersion	Grants permission to Delete the specified version of the specified policy	Write	policy* (p. 1051)		
DeleteProvisioningTemplate	Grants permission to delete a provisioning template	Write	provisioningtemplate* (p. 1052)		
DeleteProvisioningTemplateVersion	Grants permission to delete a provisioning template version	Write	provisioningtemplate* (p. 1052)		
DeleteRegistrationCode	Grants permission to delete a CA certificate registration code	Write			
DeleteRoleAlias	Grants permission to delete the specified role alias	Write	rolealias* (p. 1051)		
DeleteScheduledAudit	Grants permission to delete a scheduled audit	Write	scheduledaudit* (p. 1052)		
DeleteSecurityProfile	Grants permission to delete a Device Defender security profile	Write	securityprofile* (p. 1052) custommetric (p. 1052) dimension (p. 1052)		
DeleteStream	Grants permission to delete a specified stream	Write	stream* (p. 1052)		
DeleteThing	Grants permission to delete the specified thing	Write	thing* (p. 1051)		
DeleteThingGroup	Grants permission to delete the specified thing group	Write	thinggroup* (p. 1051)		
DeleteThingShadow	Grants permission to delete the specified thing shadow	Write	thing* (p. 1051)		
DeleteThingType	Grants permission to delete the specified thing type	Write	thingtype* (p. 1051)		
DeleteTopicRule	Grants permission to delete the specified rule	Write	rule* (p. 1052)		
DeleteTopicRuleDestination	Grants permission to delete a Topic Rule Destination	Write	destination* (p. 1052)		
DeleteV2LoggingLevel	Grants permission to delete the specified v2 logging level	Write			
DeprecateThingType	Grants permission to deprecate the specified thing type	Write	thingtype* (p. 1051)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeAccountAuditFindings	Grants permission to get information about audit configurations for the account	Read			
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			
DescribeAuditMitigationTask	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* (p. 1051)		
DescribeBillingGroup	Grants permission to get information about the specified billing group	Read	billinggroup* (p. 1051)		
DescribeCACertificate	Grants permission to describe a registered CA certificate	Read	cacert* (p. 1052)		
DescribeCertificate	Grants permission to get information about the specified certificate	Read	cert* (p. 1052)		
DescribeCustomMetric	Grants permission to describe a custom metric that is defined in your AWS account	Read	custommetric* (p. 1052)		
DescribeDefaultAuthorizer	Grants permission to describe the default authorizer	Read			
DescribeDetectMitigationAction	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* (p. 1052)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDomainConfiguration	Grants permission to get information about the domain configuration	Read	domainconfiguration* (p. 1052)		
DescribeEndpoint	Grants permission to get a unique endpoint specific to the AWS account making the call	Read			
DescribeEventConfigurations	Grants permission to get event configurations	Read			
DescribeFleetMetrics	Grants permission to get information about the specified fleet metric	Read	fleetmetric* (p. 1051)		
DescribeIndex	Grants permission to get information about the specified index	Read	index* (p. 1051)		
DescribeJob	Grants permission to describe a job	Read	job* (p. 1051)		
DescribeJobExecution	Grants permission to describe a job execution	Read	job (p. 1051) thing (p. 1051)		
DescribeJobTemplate	Grants permission to describe a job template	Read	jobtemplate* (p. 1051)		
DescribeManagedJobTemplate	Grants permission to describe a managed job template	Read	jobtemplate* (p. 1051)		
DescribeMitigationAction	Grants permission to get information about a mitigation action	Read	mitigationaction* (p. 1052)		
DescribeProvisioningTemplate	Grants permission to get information about a fleet provisioning template	Read	provisioningtemplate* (p. 1052)		
DescribeProvisioningTemplateVersion	Grants permission to get information about a fleet provisioning template version	Read	provisioningtemplate* (p. 1052)		
DescribeRoleAlias	Grants permission to describe a role alias	Read	rolealias* (p. 1051)		
DescribeScheduledAudit	Grants permission to get information about a scheduled audit	Read	scheduledaudit* (p. 1052)		
DescribeSecurityProfile	Grants permission to get information about a Device Defender security profile	Read	securityprofile* (p. 1052)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeStream	Grants permission to get information about the specified stream	Read	stream* (p. 1052)		
DescribeThing	Grants permission to get information about the specified thing	Read	thing* (p. 1051)		
DescribeThingGroup	Grants permission to get information about the specified thing group	Read	thinggroup* (p. 1051)		
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* (p. 1051)		
DescribeTunnel	Grants permission to describe a tunnel	Read	tunnel* (p. 1051)		
DetachPolicy	Grants permission to detach a policy from the specified target	Permissions management	cert (p. 1052) thinggroup (p. 1051)		
DetachPrincipalPolicy	Grants permission to remove the specified policy from the specified certificate	Permissions management	cert (p. 1052)		
DetachSecurityProfile	Grants permission to disassociate a Device Defender security profile from a thing group or from this account	Write	securityprofile* (p. 1052)		
			custommetric (p. 1052)		
			dimension (p. 1052)		
			thinggroup (p. 1051)		
DetachThingPrincipal	Grants permission to detach the specified principal from the specified thing	Write			
DisableTopicRule	Grants permission to disable the specified rule	Write	rule* (p. 1052)		
EnableTopicRule	Grants permission to enable the specified rule	Write	rule* (p. 1052)		
GetBehaviorModel	Grants permission to fetch a Device Defender ML Detect Security Profile training model's status	List	securityprofile (p. 1052)		
GetBucketsAggregation	Grants permission to get buckets aggregation for IoT fleet index	Read	index* (p. 1051)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCardinality	Grants permission to get cardinality for IoT fleet index	Read	index* (p. 1051)		
GetEffectivePolicies	Grants permission to get effective policies	Read	cert (p. 1052)		
GetIndexingConfig	Grants permission to get current indexing configuration	Read			
GetJobDocument	Grants permission to get a job document	Read	job* (p. 1051)		
GetLoggingOptions	Grants permission to get the logging options	Read			
GetOTAUpdate	Grants permission to get the information about the OTA update job	Read	otaupdate* (p. 1052)		
GetPercentiles	Grants permission to get percentiles for IoT fleet index	Read	index* (p. 1051)		
GetPolicy	Grants permission to get information about the specified policy with the policy document of the default version	Read	policy* (p. 1051)		
GetPolicyVersion	Grants permission to get information about the specified policy version	Read	policy* (p. 1051)		
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* (p. 1051)		
GetStatistics	Grants permission to get statistics for IoT fleet index	Read	index* (p. 1051)		
GetThingShadow	Grants permission to get the thing shadow	Read	thing* (p. 1051)		
GetTopicRule	Grants permission to get information about the specified rule	Read	rule* (p. 1052)		
GetTopicRuleDestination	Grants permission to get a TopicRuleDestination	Read	destination* (p. 1052)		
GetV2LoggingOptions	Grants permission to get v2 logging options	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListActiveViolations	Grants permission to list the active violations for a given Device Defender security profile or Thing	List	securityprofile (p. 1052)		
			thing (p. 1051)		
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			
ListAuditMitigationActions	Grants permission to get the status of audit mitigation action tasks that were executed	List			
ListAuditMitigationActionsAudit Mitigation Actions	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			
ListCertificates	Grants permission to list your certificates	List			
ListCertificatesByDevice	Grants permission to list the device certificates signed by the specified CA certificate	List			
ListCustomMetrics	Grants permission to list the custom metrics in your AWS account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDetectMitigationActionsExecutions	Grants permission to lists mitigation actions executions for a Device Defender ML Detect Security Profile	List	thing (p. 1051)		
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 domains configuration created by your AWS account	List			
ListFleetMetrics	Grants permission to list the fleet metrics in your account	List			
ListIndices	Grants permission to list all indices for fleet index	List			
ListJobExecutions	Grants permission to list the job executions for a job	List	job* (p. 1051)		
ListJobExecutionsForThing	Grants permission to list the job executions for the specified thing	List	thing* (p. 1051)		
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	Adds support to list metric datapoints collected for IoT devices	List	thing* (p. 1051)		
ListMitigationActions	Grants permission to get a list of mitigation actions that match the specified filter criteria	List			
ListNamedShadowsForThing	Grants permission to list all named shadows for a given thing	List	thing* (p. 1051)		
ListOTAUpdates	Grants permission to list OTA update jobs in the account	List			
ListOutgoingCertificates	Grants permission to list certificates that are being transferred but not yet accepted	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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* (p. 1051)		
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			
ListProvisioningTemplates	Grants permission to get a list of fleet provisioning template versions	List	provisioningtemplate* (p. 1052)		
ListProvisioningTemplateTargets	Grants permission to list the fleet provisioning templates in your AWS account	List			
ListRetainedMessages	Grants permission to list the retained messages for your account	List			
ListRoleAliases	Grants permission to list role aliases	List			
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 (p. 1052)		
ListSecurityProfilesForTargets	Grants permission to list the Device Defender security profiles attached to a target			dimension (p. 1052)	
ListStreams	Grants permission to list the streams in your account	List	thinggroup (p. 1051)		
ListTagsForResource	Grants permission to list all tags for a given resource	Read	authorizer (p. 1051)		
				billinggroup (p. 1051)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			cacert (p. 1052) custommetric (p. 1052) dimension (p. 1052) domainconfiguration (p. 1052) dynamicthinggroup (p. 1051) fleetmetric (p. 1051) job (p. 1051) jobtemplate (p. 1051) mitigationaction (p. 1052) otaupdate (p. 1052) policy (p. 1051) provisioningtemplate (p. 1052) rolealias (p. 1051) rule (p. 1052) scheduledaudit (p. 1052) securityprofile (p. 1052) stream (p. 1052) thinggroup (p. 1051) thingtype (p. 1051)		
ListTargetsForPolicy	Grants permission to list targets for the specified policy	List	policy* (p. 1051)		
ListTargetsForSecurityProfile	Grants permission to list the targets associated with a given Device Defender security profile	List	securityprofile* (p. 1052)		
ListThingGroups	Grants permission to list all thing groups	List			
ListThingGroupsForThing	Grants permission to list thing groups to which the specified thing belongs	List	thing* (p. 1051)		
ListThingPrincipals	Grants permission to list the principals associated with the specified thing	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListThingRegistrationReports	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* (p. 1051)		
ListThingsInThingGroup	Grants permission to list all things in the specified thing group	List	thinggroup* (p. 1051)		
ListTopicRuleDestinations	Grants permission to list all Topic Rule Destinations	List			
ListTopicRules	Grants permission to list the rules for the specific topic	List			
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 (p. 1052) thing (p. 1051)		
OpenTunnel	Grants permission to open a tunnel	Write		aws:RequestTag/\${TagKey} (p. 1053) aws:TagKeys (p. 1053) iot:ThingGroupArn (p. 1053) iot:TunnelDestinationService (p. 1053)	
Publish	Grants permission to publish to the specified topic	Write	topic* (p. 1051)		
PutVerificationState	Grants permission to put verification state on a violation	Write			
Receive	Grants permission to receive from the specified topic	Write	topic* (p. 1051)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterCACertificate	Grants permission to register a CA certificate with AWS IoT	Write		aws:RequestTag:PassRole \${TagKey} (p. 1053)	aws:TagKeys (p. 1053)
RegisterCertificate	Grants permission to register a device certificate with AWS IoT	Write			
RegisterCertificateDeviceCA	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* (p. 1052)		
RemoveThingFromBillingGroup	Grants permission to remove a thing from the specified billing group	Write	billinggroup* (p. 1051)		
RemoveThingFromThingGroup	Grants permission to remove a thing from the specified thing group		thing* (p. 1051)	thinggroup* (p. 1051)	
ReplaceTopicRule	Grants permission to replace the specified rule	Write	rule* (p. 1052)		
RetainPublish	Grants permission to publish a retained message to the specified topic	Write	topic* (p. 1051)		
RotateTunnelAccessTokens	Grants permission to rotate the access token of a tunnel	Write	tunnel* (p. 1051)		
			iot:ThingGroupArn (p. 1053)	iot:TunnelDestinationService (p. 1053)	iot:ClientMode (p. 1053)
SearchIndex	Grants permission to search IoT fleet index	Read	index* (p. 1051)		
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* (p. 1051)		
SetDefaultPolicyVersion	Grants permission to set the specified version of the specified policy as the policy's default (operative) version	Permissions management	policy* (p. 1051)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SetLoggingOptions	Grants permission to set the logging options	Write			
SetV2LoggingLevel	Grants permission to set the v2 logging level	Write			
SetV2LoggingOptions	Grants permission to set the v2 logging options	Write			
StartAuditMitigationActionsTask	Grants permission to start a task that applies a set of mitigation actions to the specified target	Write			
StartDetectMitigationActionsTask	Grants permission to start a Device Defender ML Detect mitigation actions task	Write	securityprofile (p. 1052)		
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* (p. 1051)		
TagResource	Grants permission to tag a specified resource	Tagging	authorizer (p. 1051) billinggroup (p. 1051) cacert (p. 1052) custommetric (p. 1052) dimension (p. 1052) domainconfiguration (p. 1052) dynamicthinggroup (p. 1051) fleetmetric (p. 1051) job (p. 1051) jobtemplate (p. 1051) mitigationaction (p. 1052) otaupdate (p. 1052) policy (p. 1051) provisioningtemplate (p. 1052)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			rolealias (p. 1051) rule (p. 1052) scheduledaudit (p. 1052) securityprofile (p. 1052) stream (p. 1052) thinggroup (p. 1051) thingtype (p. 1051)		aws:RequestTag/ \${TagKey} (p. 1053) aws:TagKeys (p. 1053)
TestAuthorization	Grants permission to test the policies evaluation for group policies	Read	cert (p. 1052)		
TestInvokeAuthorizer	Grants permission to test invoke the specified custom authorizer for testing purposes	Read	authorizer* (p. 1051)		
TransferCertificate	Grants permission to transfer the specified certificate to the specified AWS account	Write	cert* (p. 1052)		
UntagResource	Grants permission to untag a specified resource	Tagging	authorizer (p. 1051)		
billinggroup (p. 1051)					
cacert (p. 1052)					
custommetric (p. 1052)					
dimension (p. 1052)					
domainconfiguration (p. 1052)					
dynamicthinggroup (p. 1051)					
fleetmetric (p. 1051)					
job (p. 1051)					
jobtemplate (p. 1051)					
mitigationaction (p. 1052)					
otaupdate (p. 1052)					
policy (p. 1051)					
provisioningtemplate (p. 1052)					

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			rolealias (p. 1051) rule (p. 1052) scheduledaudit (p. 1052) securityprofile (p. 1052) stream (p. 1052) thinggroup (p. 1051) thingtype (p. 1051) aws:TagKeys (p. 1053)		
UpdateAccountAuditConfiguration	Grants permission to configure the Device Defender audit settings for this account	Write			
UpdateAuditSuppression	Grants permission to update Device Defender audit suppression	Write			
UpdateAuthorizer	Grants permission to update an authorizer	Write	authorizer* (p. 1051)		
UpdateBillingGroup	Grants permission to update information associated with the specified billing group	Write	billinggroup* (p. 1051)		
UpdateCACertificate	Grants permission to update a registered CA certificate	Write	cacert* (p. 1052)		iam:PassRole
UpdateCertificate	Grants permission to update the status of the specified certificate. This operation is idempotent	Write	cert* (p. 1052)		
UpdateCustomMetric	Grants permission to update the specified custom metric	Write	custommetric* (p. 1052)		
UpdateDimension	Grants permission to update the definition for a dimension	Write	dimension* (p. 1052)		
UpdateDomainConfiguration	Grants permission to update a domain configuration	Write	domainconfiguration* (p. 1052)		
UpdateDynamicThingGroup	Grants permission to update a Dynamic Thing Group	Write	dynamicthinggroup* (p. 1051)		
UpdateEventConfigurations	Grants permission to update event configurations	Write			
UpdateFleetMetric	Grants permission to update a fleet metric	Write	fleetmetric* (p. 1051)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			index* (p. 1051)		
UpdateIndexingConfig	Grants permission to update fleet indexing configuration	Write			
UpdateJob	Grants permission to update a job	Write	job* (p. 1051)		
UpdateMitigationAction	Grants permission to update the definition for the specified mitigation action	Write	mitigationaction* (p. 1052)		
UpdateProvisioningTemplate	Grants permission to update a fleet provisioning template	Write	provisioningtemplate* (p. 1052)		iam:PassRole
UpdateRoleAlias	Grants permission to update the role alias	Write	rolealias* (p. 1051)		iam:PassRole
UpdateScheduledAudit	Grants permission to update a scheduled audit, including what checks are performed and how often the audit takes place	Write	scheduledaudit* (p. 1052)		
UpdateSecurityProfile	Grants permission to update a Device Defender security profile	Write	securityprofile* (p. 1052)		
			custommetric (p. 1052)		
			dimension (p. 1052)		
UpdateStream	Grants permission to update the data for a stream	Write	stream* (p. 1052)		
UpdateThing	Grants permission to update information associated with the specified thing	Write	thing* (p. 1051)		
UpdateThingGroup	Grants permission to update information associated with the specified thing group	Write	thinggroup* (p. 1051)		
UpdateThingGroups	Grants permission to update the thing groups to which the thing belongs	Write	thing* (p. 1051)		
			thinggroup (p. 1051)		
UpdateThingShadow	Grants permission to update the thing shadow	Write	thing* (p. 1051)		
UpdateTopicRule	Grants permission to update a Topic Rule Destination	Write	destination* (p. 1052)		
ValidateSecurityProfile	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 \(p. 1030\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1053)
job	arn:\${Partition}:iot:\${Region}: \${Account}:job/\${JobId}	aws:ResourceTag/\${TagKey} (p. 1053)
jobtemplate	arn:\${Partition}:iot:\${Region}: \${Account}:jobtemplate/\${JobTemplateId}	aws:ResourceTag/\${TagKey} (p. 1053)
tunnel	arn:\${Partition}:iot:\${Region}: \${Account}:tunnel/\${TunnelId}	aws:ResourceTag/\${TagKey} (p. 1053)
thing	arn:\${Partition}:iot:\${Region}: \${Account}:thing/\${ThingName}	
thinggroup	arn:\${Partition}:iot:\${Region}: \${Account}:thinggroup/\${ThingGroupName}	aws:ResourceTag/\${TagKey} (p. 1053)
billinggroup	arn:\${Partition}:iot:\${Region}: \${Account}:billinggroup/\${BillingGroupName}	aws:ResourceTag/\${TagKey} (p. 1053)
dynamicthinggroup	arn:\${Partition}:iot:\${Region}: \${Account}:thinggroup/\${ThingGroupName}	aws:ResourceTag/\${TagKey} (p. 1053)
thingtype	arn:\${Partition}:iot:\${Region}: \${Account}:thingtype/\${ThingTypeName}	aws:ResourceTag/\${TagKey} (p. 1053)
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} (p. 1053)
authorizer	arn:\${Partition}:iot:\${Region}: \${Account}:authorizer/\${AuthorizerName}	aws:ResourceTag/\${TagKey} (p. 1053)
policy	arn:\${Partition}:iot:\${Region}: \${Account}:policy/\${PolicyName}	aws:ResourceTag/\${TagKey} (p. 1053)

Resource types	ARN	Condition keys
<code>cert</code>	<code>arn:\${Partition}:iot:\${Region}: \${Account}:cert/\${Certificate}</code>	
<code>cacert</code>	<code>arn:\${Partition}:iot:\${Region}: \${Account}:cacert/\${CACertificate}</code>	<code>aws:ResourceTag/ \${TagKey}</code> (p. 1053)
<code>stream</code>	<code>arn:\${Partition}:iot:\${Region}: \${Account}:stream/\${StreamId}</code>	<code>aws:ResourceTag/ \${TagKey}</code> (p. 1053)
<code>otaupdate</code>	<code>arn:\${Partition}:iot:\${Region}: \${Account}:otaupdate/\${OtaUpdateId}</code>	<code>aws:ResourceTag/ \${TagKey}</code> (p. 1053)
<code>scheduledaudit</code>	<code>arn:\${Partition}:iot:\${Region}: \${Account}:scheduledaudit/\${ScheduleName}</code>	<code>aws:ResourceTag/ \${TagKey}</code> (p. 1053)
<code>mitigationaction</code>	<code>arn:\${Partition}:iot:\${Region}: \${Account}:mitigationaction/ \${MitigationActionName}</code>	<code>aws:ResourceTag/ \${TagKey}</code> (p. 1053)
<code>securityprofile</code>	<code>arn:\${Partition}:iot:\${Region}: \${Account}:securityprofile/ \${SecurityProfileName}</code>	<code>aws:ResourceTag/ \${TagKey}</code> (p. 1053)
<code>custommetric</code>	<code>arn:\${Partition}:iot:\${Region}: \${Account}:custommetric/\${MetricName}</code>	<code>aws:ResourceTag/ \${TagKey}</code> (p. 1053)
<code>dimension</code>	<code>arn:\${Partition}:iot:\${Region}: \${Account}:dimension/\${DimensionName}</code>	<code>aws:ResourceTag/ \${TagKey}</code> (p. 1053)
<code>rule</code>	<code>arn:\${Partition}:iot:\${Region}: \${Account}:rule/\${RuleName}</code>	<code>aws:ResourceTag/ \${TagKey}</code> (p. 1053)
<code>destination</code>	<code>arn:\${Partition}:iot:\${Region}: \${Account}:destination/\${DestinationType}/ \${Uuid}</code>	
<code>provisioningtemplate</code>	<code>arn:\${Partition}:iot:\${Region}: \${Account}:provisioningtemplate/ \${ProvisioningTemplate}</code>	<code>aws:ResourceTag/ \${TagKey}</code> (p. 1053)
<code>domainconfiguration</code>	<code>arn:\${Partition}:iot:\${Region}: \${Account}:domainconfiguration/ \${DomainConfigurationName}/\${Id}</code>	<code>aws:ResourceTag/ \${TagKey}</code> (p. 1053)

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 [Available global condition 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
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:Delete	Filters access by a flag indicating whether or not to also delete an IoT Tunnel immediately when making <code>iot:CloseTunnel</code> request	Bool
iot:DomainName	Filters access by based on the domain name of an IoT DomainConfiguration	String
iot:ThingGroupArn	Filters access by a list of IoT Thing Group ARNs that the destination IoT Thing belongs to for an IoT Tunnel	String
iot:TunnelDestinationTunnel	Filters access by a list of destination services for an IoT Tunnel	String

Actions, resources, and condition keys for AWS IoT 1-Click

AWS IoT 1-Click (service prefix: `iot1click`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to [configure this service](#).
- View a list of the [API 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 1-Click \(p. 1053\)](#)
- [Resource types defined by AWS IoT 1-Click \(p. 1055\)](#)
- [Condition keys for AWS IoT 1-Click \(p. 1056\)](#)

Actions defined by AWS IoT 1-Click

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

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

policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateDeviceWithPlacement	Grants permission to associate a device to a placement	Write	project* (p. 1056)		
ClaimDevicesByClaimCode	Grants permission to claim a batch of devices with a claim code	Read			
CreatePlacement	Grants permission to create a new placement in a project	Write	project* (p. 1056)		
CreateProject	Grants permission to create a new project	Write	project* (p. 1056)		
				aws:RequestTag/\${TagKey} (p. 1056)	
				aws:TagKeys (p. 1056)	
DeletePlacement	Grants permission to delete a placement from a project	Write	project* (p. 1056)		
DeleteProject	Grants permission to delete a project	Write	project* (p. 1056)		
DescribeDevice	Grants permission to describe a device	Read	device* (p. 1056)		
DescribePlacement	Grants permission to describe a placement	Read	project* (p. 1056)		
DescribeProject	Grants permission to describe a project	Read	project* (p. 1056)		
DisassociateDeviceFromPlacement	Grants permission to disassociate a device from a placement	Write	project* (p. 1056)		
FinalizeDeviceClaim	Grants permission to finalize a device claim	Read	device* (p. 1056)		
				aws:RequestTag/\${TagKey} (p. 1056)	
				aws:TagKeys (p. 1056)	
GetDeviceMethods	Grants permission to get available methods of a device	Read	device* (p. 1056)		
GetDevicesInPlacement	Grants permission to get devices associated to a placement	Read	project* (p. 1056)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
InitiateDeviceClaim	Grants permission to initialize a device claim	Read	device* (p. 1056)		
InvokeDeviceMethod	Grants permission to invoke a device method	Write	device* (p. 1056)		
ListDeviceEvents	Grants permission to list past events published by a device	Read	device* (p. 1056)		
ListDevices	Grants permission to list all devices	List			
ListPlacements	Grants permission to list placements in a project	Read	project* (p. 1056)		
ListProjects	Grants permission to list all projects	List			
ListTagsForResource	Grants permission to lists the tags for a resource	Read	device (p. 1056) project (p. 1056)		
TagResource	Grants permission to add or modify the tags of a resource	Tagging	device (p. 1056) project (p. 1056) aws:RequestTag/ \${TagKey} (p. 1056) aws:TagKeys (p. 1056)		
UnclaimDevice	Grants permission to unclaim a device	Read	device* (p. 1056)		
UntagResource	Grants permission to remove the given tags (metadata) from a resource	Tagging	device (p. 1056) project (p. 1056) aws:TagKeys (p. 1056)		
UpdateDeviceState	Grants permission to update device state	Write	device* (p. 1056)		
UpdatePlacement	Grants permission to update a placement	Write	project* (p. 1056)		
UpdateProject	Update a project	Write	project* (p. 1056)		

Resource types defined by AWS IoT 1-Click

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the [Actions table](#) (p. 1053) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
device	arn:\${Partition}:iot1click:\${Region}:\${Account}:devices/\${DeviceId}	aws:ResourceTag/\${TagKey} (p. 1056)
project	arn:\${Partition}:iot1click:\${Region}:\${Account}:projects/\${ProjectName}	aws:ResourceTag/\${TagKey} (p. 1056)

Condition keys for AWS IoT 1-Click

AWS IoT 1-Click defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see [Condition keys table](#).

To view the global condition keys that are available to all services, see [Available global condition 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 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 \(p. 1056\)](#)
- [Resource types defined by AWS IoT Analytics \(p. 1059\)](#)
- [Condition keys for AWS IoT Analytics \(p. 1060\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1059)		
CancelPipelineReprocessing	Cancels reprocessing for the specified pipeline	Write	pipeline* (p. 1060)		
CreateChannel	Creates a channel	Write	channel* (p. 1059)		
				aws:RequestTag/ \${TagKey} (p. 1060) aws:TagKeys (p. 1060)	
CreateDataset	Creates a dataset	Write	dataset* (p. 1060)		
				aws:RequestTag/ \${TagKey} (p. 1060)	
				aws:TagKeys (p. 1060)	
CreateDatasetContent	Generates content from the specified dataset (by executing the dataset actions)	Write	dataset* (p. 1060)		
CreateDatastore	Creates a datastore	Write	datastore* (p. 1060)		
				aws:RequestTag/ \${TagKey} (p. 1060)	
				aws:TagKeys (p. 1060)	
CreatePipeline	Creates a pipeline	Write	pipeline* (p. 1060)		
				aws:RequestTag/ \${TagKey} (p. 1060) aws:TagKeys (p. 1060)	
DeleteChannel	Deletes the specified channel	Write	channel* (p. 1059)		
DeleteDataset	Deletes the specified dataset	Write	dataset* (p. 1060)		
DeleteDatasetContent	Deletes the content of the specified dataset	Write	dataset* (p. 1060)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteDatastore	Deletes the specified datastore	Write	datastore* (p. 1060)		
DeletePipeline	Deletes the specified pipeline	Write	pipeline* (p. 1060)		
DescribeChannel	Describes the specified channel	Read	channel* (p. 1059)		
DescribeDataset	Describes the specified dataset	Read	dataset* (p. 1060)		
DescribeDatastore	Describes the specified datastore	Read	datastore* (p. 1060)		
DescribeLoggingOptions	Describes logging options for the account	Read			
DescribePipeline	Describes the specified pipeline	Read	pipeline* (p. 1060)		
GetDatasetContent	Gets the content of the specified dataset	Read	dataset* (p. 1060)		
ListChannels	Lists the channels for the account	List			
ListDatasetContents	Lists information about dataset contents that have been created	List	dataset* (p. 1060)		
ListDatasets	Lists the datasets for the account	List			
ListDatastores	Lists the datastores for the account	List			
ListPipelines	Lists the pipelines for the account	List			
ListTagsForResource	Lists the tags (metadata) which you have assigned to the resource	Read	channel (p. 1059) dataset (p. 1060) datastore (p. 1060) pipeline (p. 1060)		
PutLoggingOptions	Puts logging options for the account	Write			
RunPipelineActivity	Runs the specified pipeline activity	Read			
SampleChannelData	Samples the specified channel's data	Read	channel* (p. 1059)		
StartPipelineReprocessing	Starts reprocessing for the specified pipeline	Write	pipeline* (p. 1060)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Adds to or modifies the tags of the given resource. Tags are metadata which can be used to manage a resource	Tagging	channel (p. 1059) dataset (p. 1060) datastore (p. 1060) pipeline (p. 1060)	aws:RequestTag/\${TagKey} (p. 1060) aws:TagKeys (p. 1060)	
UntagResource	Removes the given tags (metadata) from the resource	Tagging	channel (p. 1059) dataset (p. 1060) datastore (p. 1060) pipeline (p. 1060)	aws:RequestTag/\${TagKey} (p. 1060) aws:TagKeys (p. 1060)	
UpdateChannel	Updates the specified channel	Write	channel* (p. 1059)		
UpdateDataset	Updates the specified dataset	Write	dataset* (p. 1060)		
UpdateDatastore	Updates the specified datastore	Write	datastore* (p. 1060)		
UpdatePipeline	Updates the specified pipeline	Write	pipeline* (p. 1060)		

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 \(p. 1056\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
channel	<code>arn:\${Partition}:iotanalytics:\${Region}: \${Account}:channel/\${ChannelName}</code>	aws:RequestTag/\${TagKey} (p. 1060) aws:TagKeys (p. 1060)

Resource types	ARN	Condition keys
		iotanalytics:ResourceTag/\${TagKey} (p. 1060)
dataset	<code>arn:\${Partition}:iotanalytics:\${Region}:\${Account}:dataset/\${DatasetName}</code>	aws:RequestTag/\${TagKey} (p. 1060) aws:TagKeys (p. 1060) iotanalytics:ResourceTag/\${TagKey} (p. 1060)
datastore	<code>arn:\${Partition}:iotanalytics:\${Region}:\${Account}:datastore/\${DatastoreName}</code>	aws:RequestTag/\${TagKey} (p. 1060) aws:TagKeys (p. 1060) iotanalytics:ResourceTag/\${TagKey} (p. 1060)
pipeline	<code>arn:\${Partition}:iotanalytics:\${Region}:\${Account}:pipeline/\${PipelineName}</code>	aws:RequestTag/\${TagKey} (p. 1060) aws:TagKeys (p. 1060) iotanalytics:ResourceTag/\${TagKey} (p. 1060)

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 [Available global condition 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 \(p. 1061\)](#)
- [Resource types defined by AWS IoT Core Device Advisor \(p. 1062\)](#)
- [Condition keys for AWS IoT Core Device Advisor \(p. 1063\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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} (p. 1063) aws:TagKeys (p. 1063)	
DeleteSuiteDefinition	Grants permission to delete a suite definition	Write	Suitedefinition* (p. 1062)		
GetEndpoint	Grants permission to get a Device Advisor endpoint	Read			
GetSuiteDefinition	Grants permission to get a suite definition	Read	Suitedefinition* (p. 1062)		
GetSuiteRun	Grants permission to get a suite run	Read	Suiterun* (p. 1062)		
GetSuiteRunReport	Grants permission to get the qualification report for a suite run	Read	Suiterun* (p. 1062)		
ListSuiteDefinitions	Grants permission to list suite definitions	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListSuiteRuns	Grants permission to list suite runs	List	Suitedefinition* (p. 1062)		
ListTagsForResource	Grants permission to list the tags (metadata) assigned to a resource	Read	Suitedefinition (p. 1062)		
			Suiterun (p. 1062)		
StartSuiteRun	Grants permission to start a suite run	Write		aws:RequestTag/\${TagKey} (p. 1063) aws:TagKeys (p. 1063)	
StopSuiteRun	Grants permission to stop a suite run	Write	Suiterun* (p. 1062)		
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 (p. 1062)		
			Suiterun (p. 1062)		
				aws:RequestTag/\${TagKey} (p. 1063) aws:TagKeys (p. 1063)	
UntagResource	Grants permission to remove the given tags (metadata) from a resource	Tagging	Suitedefinition (p. 1062)		
			Suiterun (p. 1062)		
				aws:TagKeys (p. 1063)	
UpdateSuiteDefinition	Grants permission to update a suite definition	Write	Suitedefinition* (p. 1062)		

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 \(p. 1061\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
Suitedefinition	<code>arn:\${Partition}:iotdeviceadvisor:\${Region}:\${Account}:suitedefinition/\${SuiteDefinitionId}</code>	aws:ResourceTag/\${TagKey} (p. 1063)
Suiterun	<code>arn:\${Partition}:iotdeviceadvisor:\${Region}:\${Account}:suiterun/\${SuiteDefinitionId}/\${SuiteRunId}</code>	aws:ResourceTag/\${TagKey} (p. 1063)

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 [Available global condition 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 Core for LoRaWAN

AWS IoT Core for LoRaWAN (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 Core for LoRaWAN \(p. 1063\)](#)
- [Resource types defined by AWS IoT Core for LoRaWAN \(p. 1071\)](#)
- [Condition keys for AWS IoT Core for LoRaWAN \(p. 1072\)](#)

Actions defined by AWS IoT Core for LoRaWAN

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

The **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateAwsAccountWithRegion	Grants permission to link AWS account with AWS account	Write		aws:RequestTag/\${TagKey} (p. 1072) aws:TagKeys (p. 1072)	
AssociateMulticastGroupWithFuotaTask	Grants permission to associate the MulticastGroup with FuotaTask	Write	FuotaTask* (p. 1072)		
			MulticastGroup* (p. 1072)		
AssociateWirelessDeviceWithFuotaTask	Grants permission to associate the wireless device with FuotaTask	Write	FuotaTask* (p. 1072)		
			WirelessDevice* (p. 1071)		
AssociateWirelessDeviceWithMulticastGroup	Grants permission to associate the WirelessDevice with MulticastGroup	Write	MulticastGroup* (p. 1072)		
			WirelessDevice* (p. 1071)		
AssociateWirelessThingWithWirelessDevice	Grants permission to associate the wireless device with AWS IoT thing for a given wirelessDeviceId	Write	WirelessDevice* (p. 1071)	iot:DescribeThing	
			thing* (p. 1072)		
AssociateWirelessGatewayWithCoreIdentity	Grants permission to associate the wireless gateway with the IoT Core Identity certificate	Write	WirelessGateway* (p. 1071)		
			cert* (p. 1072)		
AssociateWirelessGatewayWithThing	Grants permission to associate the wireless gateway with AWS IoT thing for a given wirelessGatewayId	Write	WirelessGateway* (p. 1071)	iot:DescribeThing	
			thing* (p. 1072)		
CancelMulticastGroupSession	Grants permission to cancel the MulticastGroup session	Write	MulticastGroup* (p. 1072)		
CreateDestination	Grants permission to create a Destination resource	Write		aws:RequestTag/\${TagKey} (p. 1072) aws:TagKeys (p. 1072)	
CreateDeviceProfile	Grants permission to create a DeviceProfile resource	Write		aws:RequestTag/\${TagKey} (p. 1072) aws:TagKeys (p. 1072)	
CreateFuotaTask	Grants permission to create a FuotaTask resource	Write		aws:RequestTag/\${TagKey} (p. 1072) aws:TagKeys (p. 1072)	
CreateMulticastGroup	Grants permission to create a MulticastGroup resource	Write		aws:RequestTag/\${TagKey} (p. 1072) aws:TagKeys (p. 1072)	
CreateNetworkAnalyzerConfiguration		Write	WirelessDevice* (p. 1071)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateNetworkAnalyzerConfiguration	Grants permission to create a NetworkAnalyzerConfiguration resource		WirelessGateway* (p. 1071)		
			aws:RequestTag/ \${TagKey} (p. 1072)		aws:TagKeys (p. 1072)
CreateServiceProfile	Grants permission to create a ServiceProfile resource	Write		aws:RequestTag/ \${TagKey} (p. 1072)	aws:TagKeys (p. 1072)
CreateWirelessDevice	Grants permission to create a WirelessDevice resource with given Destination	Write		aws:RequestTag/ \${TagKey} (p. 1072)	aws:TagKeys (p. 1072)
CreateWirelessGateway	Grants permission to create a WirelessGateway resource	Write		aws:RequestTag/ \${TagKey} (p. 1072)	aws:TagKeys (p. 1072)
CreateWirelessGatewayTask	Grants permission to create a task definition for a given WirelessGateway	Write	WirelessGateway* (p. 1071)		
CreateWirelessGatewayTaskDefinition	Grants permission to create a WirelessGateway task definition	Write		aws:RequestTag/ \${TagKey} (p. 1072)	aws:TagKeys (p. 1072)
DeleteDestination	Grants permission to delete a Destination	Write	Destination* (p. 1072)		
DeleteDeviceProfile	Grants permission to delete a DeviceProfile	Write	DeviceProfile* (p. 1071)		
DeleteFuotaTask	Grants permission to delete the FuotaTask	Write	FuotaTask* (p. 1072)		
DeleteMulticastGroup	Grants permission to delete the MulticastGroup	Write	MulticastGroup* (p. 1072)		
DeleteNetworkAnalyzerConfiguration	Grants permission to delete the NetworkAnalyzerConfiguration	Write	NetworkAnalyzerConfiguration* (p. 1072)		
DeleteQueuedMessage	Grants permission to delete the QueuedMessages	Write			
DeleteServiceProfile	Grants permission to delete a ServiceProfile	Write	ServiceProfile* (p. 1071)		
DeleteWirelessDevice	Grants permission to delete a WirelessDevice	Write	WirelessDevice* (p. 1071)		
DeleteWirelessGateway	Grants permission to delete a WirelessGateway	Write	WirelessGateway* (p. 1071)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteWirelessGateway	Grants permission to delete task for a given WirelessGateway	Write	WirelessGateway* (p. 1071)		
DeleteWirelessGatewayTaskDefinition	Grants permission to delete a WirelessGateway task definition	Write	WirelessGatewayTaskDefinition* (p. 1072)		
DisassociateAwsAccountFromPartnerAccount	Grants permission to disassociate an AWS account from a partner account	Write	SidewalkAccount* (p. 1072)		
DisassociateMulticastGroupFromFuotaTask	Grants permission to disassociate the MulticastGroup from FuotaTask	Write	FuotaTask* (p. 1072)		
			MulticastGroup* (p. 1072)		
DisassociateWirelessDeviceFromFuotaTask	Grants permission to disassociate the Wireless device from FuotaTask	Write	FuotaTask* (p. 1072)		
			WirelessDevice* (p. 1071)		
DisassociateWirelessDeviceFromMulticastGroup	Grants permission to disassociate the Wireless device from MulticastGroup	Write	MulticastGroup* (p. 1072)		
			WirelessDevice* (p. 1071)		
DisassociateWirelessDeviceFromThing	Grants permission to disassociate a Wireless device from a AWS IoT thing	Write	WirelessDevice* (p. 1071)	iot:DescribeThing	
			thing* (p. 1072)		
DisassociateWirelessGatewayFromIdentityCertificate	Grants permission to disassociate a WirelessGateway from a IoT Core Identity certificate	Write	WirelessGateway* (p. 1071)		
			cert* (p. 1072)		
DisassociateWirelessGatewayFromThing	Grants permission to disassociate a WirelessGateway from a IoT Core thing	Write	WirelessGateway* (p. 1071)	iot:DescribeThing	
			thing* (p. 1072)		
GetDestination	Grants permission to get the Destination	Read	Destination* (p. 1072)		
GetDeviceProfile	Grants permission to get the DeviceProfile	Read	DeviceProfile* (p. 1071)		
GetEventConfigurationsByResourceTypes	Grants permission to get event configurations by Resource types	Read			
GetFuotaTask	Grants permission to get the FuotaTask	Read	FuotaTask* (p. 1072)		
GetLogLevelByResourceType	Grants permission to get log levels by resource types	Read			
GetMulticastGroup	Grants permission to get the MulticastGroup	Read	MulticastGroup* (p. 1072)		
GetMulticastGroupSession	Grants permission to get the MulticastGroup session	Read	MulticastGroup* (p. 1072)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetNetworkAnalyzerConfiguration	Grants permission to get the NetworkAnalyzerConfiguration	Read	NetworkAnalyzerConfiguration* (p. 1072)		
GetPartnerAccount	Grants permission to get the associated PartnerAccount	Read	SidewalkAccount* (p. 1072)		
GetResourceEventConfigurations	Grants permission to get an Event configuration for an identifier	Read	SidewalkAccount (p. 1072)		
			WirelessDevice (p. 1071)		
			WirelessGateway (p. 1071)		
GetResourceLogLevel	Grants permission to get resource log level	Read	WirelessDevice (p. 1071)		
			WirelessGateway (p. 1071)		
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* (p. 1071)		
GetWirelessDevice	Grants permission to get the WirelessDevice	Read	WirelessDevice* (p. 1071)		
GetWirelessDeviceStatistics	Grants permission to get the WirelessDevice statistics info for a given WirelessDevice	Read	WirelessDevice* (p. 1071)		
GetWirelessGateway	Grants permission to get the WirelessGateway	Read	WirelessGateway* (p. 1071)		
GetWirelessGatewayIdentity	Grants permission to get the WirelessGateway identity certificate id associated with the WirelessGateway	Read	WirelessGateway* (p. 1071)		
GetWirelessGatewayInfo	Grants permission to get Currentfirmwareversion and other information for the WirelessGateway	Read	WirelessGateway* (p. 1071)		
GetWirelessGatewayStatistics	Grants permission to get Statisticsinfo for a given WirelessGateway	Read	WirelessGateway* (p. 1071)		
GetWirelessGatewayTask	Grants permission to get the task for a given WirelessGateway	Read	WirelessGateway* (p. 1071)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetWirelessGatewayTaskDefinition	Grants permission to get the given WirelessGateway task definition	Read	WirelessGatewayTaskDefinition* (p. 1072)		
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			
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			
ListMulticastGroupInformation	Grants permission to list information of available MulticastGroups by FuotaTask based on the AWS account	Read	FuotaTask* (p. 1072)		
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			
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 (p. 1072)		
			DeviceProfile (p. 1071)		
			NetworkAnalyzerConfiguration (p. 1072)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ServiceProfile (p. 1071) SidewalkAccount (p. 1072) WirelessDevice (p. 1071) WirelessGateway (p. 1071)		
			WirelessGatewayTaskDefinition (p. 1072)		
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			
ListWirelessGateways	Grants permission to list information of available WirelessGateways based on the AWS account	Read			
PutResourceLogLevel	Grants permission to put resource log level	Write	WirelessDevice (p. 1071)		
ResetAllResourceLogLevels	Grants permission to reset all resource log levels		WirelessGateway (p. 1071)		
ResetResourceLogLevel	Grants permission to reset resource log level	Write	WirelessDevice (p. 1071)	WirelessGateway (p. 1071)	
SendDataToMulticastGroup	Grants permission to send data to the MulticastGroup	Write	MulticastGroup* (p. 1072)		
SendDataToWirelessDevice	Grants permission to send the decrypted application data frame to the target device	Write	WirelessDevice* (p. 1071)		
StartBulkAssociateWirelessDevicesWithMulticastGroup	Grants permission to associate the WirelessDevicesWithMulticastGroup MulticastGroup	Write	MulticastGroup* (p. 1072)		
StartBulkDisassociateWirelessDevicesFromMulticastGroup	Grants permission to bulk disassociate the WirelessDevicesFromMulticastGroup from MulticastGroup	Write	MulticastGroup* (p. 1072)		
StartFuotaTask	Grants permission to start the FuotaTask	Write	FuotaTask* (p. 1072)		
StartMulticastGroupSession	Grants permission to start the MulticastGroup session	Write	MulticastGroup* (p. 1072)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartNetworkAnalyzer	Grants permission to start Network Analyzer stream	Write	NetworkAnalyzerConfiguration* (p. 1072)		
TagResource	Grants permission to tag a given resource	Tagging	Destination (p. 1072) DeviceProfile (p. 1071) NetworkAnalyzerConfiguration (p. 1072) ServiceProfile (p. 1071) SidewalkAccount (p. 1072) WirelessDevice (p. 1071) WirelessGateway (p. 1071) WirelessGatewayTaskDefinition (p. 1072)		
TestWirelessDevice	Grants permission to simulate a provisioned device to send an uplink data with payload of 'Hello'	Write	WirelessDevice* (p. 1071)		
UntagResource	Grants permission to remove the given tags from the resource	Tagging	Destination (p. 1072) DeviceProfile (p. 1071) NetworkAnalyzerConfiguration (p. 1072) ServiceProfile (p. 1071) SidewalkAccount (p. 1072) WirelessDevice (p. 1071) WirelessGateway (p. 1071) WirelessGatewayTaskDefinition (p. 1072)		
UpdateDestination	Grants permission to update a Destination resource	Write	Destination* (p. 1072)		
UpdateEventConfigurations	Grants permission to update event configurations by resource types	Write			
UpdateFuotaTask	Grants permission to update the FuotaTask	Write	FuotaTask* (p. 1072)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateLogLevelByResourceType	Grants permission to update log levels by resource types	Write			
UpdateMulticastGroup	Grants permission to update the MulticastGroup	Write	MulticastGroup* (p. 1072)		
UpdateNetworkAnalyzerConfiguration	Grants permission to update the NetworkAnalyzerConfiguration	Write	NetworkAnalyzerConfiguration* (p. 1072)		
			WirelessDevice* (p. 1071)		
			WirelessGateway* (p. 1071)		
UpdatePartnerAccount	Grants permission to update a partner account	Write	SidewalkAccount* (p. 1072)		
UpdateResourceEntryConfiguration	Grants permission to update a resource entry configuration for an identifier	Write	SidewalkAccount (p. 1072)		
			WirelessDevice (p. 1071)		
			WirelessGateway (p. 1071)		
UpdateWirelessDevice	Grants permission to update a WirelessDevice resource	Write	WirelessDevice* (p. 1071)		
UpdateWirelessGateway	Grants permission to update a WirelessGateway resource	Write	WirelessGateway* (p. 1071)		

Resource types defined by AWS IoT Core for LoRaWAN

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the [Actions table](#) (p. 1063) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1072)
WirelessGateway	arn:\${Partition}:iotwireless:\${Region}:\${Account}:WirelessGateway/\${WirelessGatewayId}	aws:ResourceTag/\${TagKey} (p. 1072)
DeviceProfile	arn:\${Partition}:iotwireless:\${Region}:\${Account}:DeviceProfile/\${DeviceProfileId}	aws:ResourceTag/\${TagKey} (p. 1072)
ServiceProfile	arn:\${Partition}:iotwireless:\${Region}:\${Account}:ServiceProfile/\${ServiceProfileId}	aws:ResourceTag/\${TagKey} (p. 1072)

Resource types	ARN	Condition keys
Destination	arn:\${Partition}:iotwireless:\${Region}: \${Account}:Destination/\${DestinationName}	aws:ResourceTag/ \${TagKey} (p. 1072)
SidewalkAccount	arn:\${Partition}:iotwireless: \${Region}: \${Account}:SidewalkAccount/ \${SidewalkAccountId}	aws:ResourceTag/ \${TagKey} (p. 1072)
WirelessGatewayTaskDefinition	arn:\${Partition}:iotwireless:\${Region}: \${TaskDefinition}:WirelessGatewayTaskDefinition/ \${WirelessGatewayTaskDefinitionId}	aws:ResourceTag/ \${TagKey} (p. 1072)
FuotaTask	arn:\${Partition}:iotwireless:\${Region}: \${Account}:FuotaTask/\${FuotaTaskId}	aws:ResourceTag/ \${TagKey} (p. 1072)
MulticastGroup	arn:\${Partition}:iotwireless: \${Region}: \${Account}:MulticastGroup/ \${MulticastGroupId}	aws:ResourceTag/ \${TagKey} (p. 1072)
NetworkAnalyzerConfiguration	arn:\${Partition}:iotwireless:\${Region}: \${Account}:NetworkAnalyzerConfiguration/ \${NetworkAnalyzerConfigurationName}	aws:ResourceTag/ \${TagKey} (p. 1072)
thing	arn:\${Partition}:iot:\${Region}: \${Account}:thing/\${ThingName}	
cert	arn:\${Partition}:iot:\${Region}: \${Account}:cert/\${Certificate}	

Condition keys for AWS IoT Core for LoRaWAN

AWS IoT Core for LoRaWAN defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see [Condition keys table](#).

To view the global condition keys that are available to all services, see [Available global condition 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
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

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 \(p. 1073\)](#)
- [Resource types defined by AWS IoT Device Tester \(p. 1074\)](#)
- [Condition keys for AWS IoT Device Tester \(p. 1074\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 for IoT Device Tester to check if a given set of product, test suite and device tester version are compatible	Read			
DownloadTestSuite	Grants permission for IoT Device Tester to download compatible test suite versions	Read			
LatestIdt	Grants permission for IoT Device Tester to get information on latest version of device tester available	Read			
SendMetrics	Grants permissions for IoT Device Tester to send usage metrics on your behalf	Write			
SupportedVersion	Grants permission for 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 [Available keys for conditions](#).

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 \(p. 1074\)](#)
- [Resource types defined by AWS IoT Events \(p. 1077\)](#)
- [Condition keys for AWS IoT Events \(p. 1078\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources (“`*`”) in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchAcknowledge or More	Grants permission to send one or more acknowledge action requests to AWS IoT Events	Write	alarmModel* (p. 1078)		

Service Authorization Reference
Service Authorization Reference
AWS IoT Events

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchDeleteDetectorModel	Grants permission to delete a detector instance within the AWS IoT Events system	Write	detectorModel* (p. 1078)		
BatchDisableAlarm	Grants permission to disable one or more alarm instances	Write	alarmModel* (p. 1078)		
BatchEnableAlarm	Grants permission to enable one or more alarm instances	Write	alarmModel* (p. 1078)		
BatchPutMessage	Grants permission to send a set of messages to the AWS IoT Events system	Write	input* (p. 1078)		
BatchResetAlarm	Grants permission to reset one or more alarm instances	Write	alarmModel* (p. 1078)		
BatchSnoozeAlarm	Grants permission to change one or more alarm instances to the snooze mode	Write	alarmModel* (p. 1078)		
BatchUpdateDetectorModel	Grants permission to update a detector instance within the AWS IoT Events system	Write	detectorModel* (p. 1078)		
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* (p. 1078)		
CreateDetectorModel	Grants permission to create a detector model to monitor an AWS IoT Events input attribute		aws:RequestTag/ \${TagKey} (p. 1078) aws:TagKeys (p. 1078)		
CreateInput	Grants permission to create an Input in IoTEvents	Write	input* (p. 1078)		
			aws:RequestTag/ \${TagKey} (p. 1078) aws:TagKeys (p. 1078)		
DeleteAlarmModel	Grants permission to delete an alarm model		alarmModel* (p. 1078)		
DeleteDetectorModel	Grants permission to delete a detector model	Write	detectorModel* (p. 1078)		
DeleteInput	Grants permission to delete an input	Write	input* (p. 1078)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeAlarm	Grants permission to retrieve information about an alarm instance	Read	alarmModel* (p. 1078)		
DescribeAlarmModel	Grants permission to retrieve information about an alarm model	Read	alarmModel* (p. 1078)		
DescribeDetector	Grants permission to retrieve information about a detector instance	Read	detectorModel* (p. 1078)		
DescribeDetectorModel	Grants permission to retrieve information about a detector model	Read	detectorModel* (p. 1078)		
DescribeDetectorModelAnalysis	Grants permission to retrieve the detector model analysis information	Read			
DescribeInput	Grants permission to retrieve an information about Input	Read	input* (p. 1078)		
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* (p. 1078)		
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* (p. 1078)		
ListDetectorModelVersions	Grants permission to list all the versions of a detector model	List	detectorModel* (p. 1078)		
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* (p. 1078)		
ListInputRoutings	Grants permission to list one or more input routings	List			
ListInputs	Grants permission to lists the inputs you have created	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to list the tags (metadata) which you have assigned to the resource	Read	alarmModel (p. 1078)		
			detectorModel (p. 1078)		
			input (p. 1078)		
PutLoggingOptions	Grants permission to set or update the AWS IoT Events logging options	Write			
StartDetectorModel	Grants permission to start the detector model analysis	Write			
TagResource	Grants permission to adds to or modifies the tags of the given resource.Tags are metadata which can be used to manage a resource	Tagging	alarmModel (p. 1078)		
			detectorModel (p. 1078)		
			input (p. 1078)		
			aws:RequestTag/ \${TagKey} (p. 1078)		
			aws:TagKeys (p. 1078)		
UntagResource	Grants permission to remove the given tags (metadata) from the resource	Tagging	alarmModel (p. 1078)		
			detectorModel (p. 1078)		
			input (p. 1078)		
			aws:TagKeys (p. 1078)		
UpdateAlarmModel	Grants permission to update an alarm model	Write	alarmModel* (p. 1078)		
UpdateDetectorModel	Grants permission to update a detector model	Write	detectorModel* (p. 1078)		
UpdateInput	Grants permission to update an input	Write	input* (p. 1078)		
UpdateInputRouting	Grants permission to update input routing	Write	input* (p. 1078)		

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 \(p. 1074\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1078)
alarmModel	arn:\${Partition}:iotevents:\${Region}:\${Account}:alarmModel/\${AlarmModelName}	aws:ResourceTag/\${TagKey} (p. 1078)
input	arn:\${Partition}:iotevents:\${Region}:\${Account}:input/\${InputName}	aws:ResourceTag/\${TagKey} (p. 1078)

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 [Available global condition 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 instanceld (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 \(p. 1079\)](#)
- [Resource types defined by AWS IoT Fleet Hub for Device Management \(p. 1080\)](#)
- [Condition keys for AWS IoT Fleet Hub for Device Management \(p. 1080\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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} (p. 1080) sso:DescribeRegisteredRe aws:TagKeys (p. 1080)	Tag/ CreateManagedAppli
DeleteApplication	Grants permission to delete an application	Write	application* (p. 1080)		sso:DeleteManagedAppli
DescribeApplication	Grants permission to describe an application	Read	application* (p. 1080)		
ListApplications	Grants permission to list all applications	List			
ListTagsForResource	Grants permission to list all tags for a resource	Read	application (p. 1080)		
TagResource	Grants permission to tag a resource	Tagging	application (p. 1080)		
				aws:TagKeys (p. 1080)	
				aws:RequestTag/ \${TagKey} (p. 1080)	
UntagResource	Grants permission to untag a resource	Tagging	application (p. 1080)		
				aws:TagKeys (p. 1080)	
UpdateApplication	Grants permission to update an application	Write	application* (p. 1080)		

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 \(p. 1079\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
application	<code>arn:\${Partition}:iotfleethub:\${Region}:\${Account}:application/\${ApplicationId}</code>	aws:ResourceTag/\${TagKey} (p. 1080)

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 [Available global condition 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 \(p. 1081\)](#)
- [Resource types defined by AWS IoT FleetWise \(p. 1084\)](#)
- [Condition keys for AWS IoT FleetWise \(p. 1084\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateVehicle	Grants permission to associate the given vehicle to a fleet	Write	fleet* (p. 1084)		
			vehicle* (p. 1084)		
CreateCampaign	Grants permission to create a campaign	Write	fleet* (p. 1084)		
			signalcatalog* (p. 1084)		
			vehicle* (p. 1084)		
CreateDecoderManifest	Grants permission to create a decoder manifest for an existing model	Write	modelmanifest* (p. 1084)		
CreateFleet	Grants permission to create a fleet	Write	signalcatalog* (p. 1084)		
CreateModelManifest	Grants permission to create a model manifest definition	Write	signalcatalog* (p. 1084)		
CreateSignalCatalog	Grants permission to create a signal catalog	Write			
CreateVehicle	Grants permission to create a vehicle	Write	decodermanifest* (p. 1084)	iot:CreateThing iot:DescribeThing	
			modelmanifest* (p. 1084)		
DeleteCampaign	Grants permission to delete a campaign	Write	campaign* (p. 1084)		
DeleteDecoderManifest	Grants permission to delete the given decoder manifest	Write	decodermanifest* (p. 1084)		
DeleteFleet	Grants permission to delete a fleet	Write	fleet* (p. 1084)		

Service Authorization Reference
Service Authorization Reference
AWS IoT FleetWise

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteModelManifest	Grants permission to delete the given model manifest	Write	modelmanifest* (p. 1084)		
DeleteSignalCatalog	Grants permission to delete a specific signal catalog	Write	signalcatalog* (p. 1084)		
DeleteVehicle	Grants permission to delete a vehicle	Write	vehicle* (p. 1084)		
DisassociateVehicle	Grants permission to disassociate a vehicle from an existing fleet	Write	fleet* (p. 1084)		
			vehicle* (p. 1084)		
GetCampaign	Grants permission to get summary information for a given campaign	Read	campaign* (p. 1084)		
GetDecoderManifest	Grants permission to get summary information for a given decoder manifest definition	Read	decodermanifest* (p. 1084)		
GetFleet	Grants permission to get summary information for a fleet	Read	fleet* (p. 1084)		
GetModelManifest	Grants permission to get summary information for a given model manifest definition	Read	modelmanifest* (p. 1084)		
GetRegisterAccountCounts	Grants permission to get the registration status with IoT FleetWise	Read			
GetSignalCatalog	Grants permission to get summary information for a specific signal catalog	Read	signalcatalog* (p. 1084)		
GetVehicle	Grants permission to get summary information for a vehicle	Read	vehicle* (p. 1084)		
GetVehicleStatus	Grants permission to get the status of the campaigns running on a specific vehicle	Read	vehicle* (p. 1084)		
ImportDecoderManifest	Grants permission to import an existing decoder manifest	Write			
ImportSignalCatalog	Grants permission to create a signal catalog by importing existing definitions	Write			
ListCampaigns	Grants permission to list campaigns	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDecoderManifestNetworkInterfaces	Grants permission to list network interfaces associated to the existing decoder manifest	List	decodermanifest* (p. 1084)		
ListDecoderManifestSignals	Grants permission to list decoder manifest signals	List	decodermanifest* (p. 1084)		
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* (p. 1084)		
ListModelManifests	Grants permission to list all nodes for the given model manifest	List	modelmanifest* (p. 1084)		
ListModelManifestsNodes	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* (p. 1084)		
ListSignalCatalogs	Grants permission to list all signal catalogs	Read			
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* (p. 1084)		
RegisterAccount	Grants permission to register an AWS account to IoT FleetWise	Write			iam:PassRole
UpdateCampaign	Grants permission to update the given campaign	Write	campaign* (p. 1084)		
UpdateDecoderManifest	Grants permission to update a decoder manifest definition	Write	decodermanifest* (p. 1084)		
UpdateFleet	Grants permission to update the fleet	Write	fleet* (p. 1084)		
UpdateModelManifest	Grants permission to update the given model manifest definition	Write	modelmanifest* (p. 1084)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateSignalCatalog	Grants permission to update a specific signal catalog definition	Write	signalcatalog* (p. 1084)		
UpdateVehicle	Grants permission to update the vehicle	Write	vehicle* (p. 1084)		
			decodermanifest (p. 1084)		
			modelmanifest (p. 1084)		
			iotfleetwise:UpdateToModelManifestA		
					iotfleetwise:UpdateToDecoderManifes

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 \(p. 1081\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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}	
decodermanifest	arn:\${Partition}:iotfleetwise:\${Region}: \${Account}:decoder-manifest/\${Name}	
fleet	arn:\${Partition}:iotfleetwise:\${Region}: \${Account}:fleet/\${FleetId}	
modelmanifest	arn:\${Partition}:iotfleetwise:\${Region}: \${Account}:model-manifest/\${Name}	
signalcatalog	arn:\${Partition}:iotfleetwise:\${Region}: \${Account}:signal-catalog/\${Name}	
vehicle	arn:\${Partition}:iotfleetwise:\${Region}: \${Account}:vehicle/\${VehicleId}	

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 [Available global condition keys](#).

Condition keys	Description	Type
iotfleetwise:UpdateToDecoderManifestArn	Filters access by a list of IoT FleetWise Decoder Manifest ARNs	String
iotfleetwise:UpdateToModelManifestArn	Filters access by a list of IoT FleetWise Model Manifest ARNs	String

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 \(p. 1085\)](#)
- [Resource types defined by AWS IoT Greengrass \(p. 1093\)](#)
- [Condition keys for AWS IoT Greengrass \(p. 1095\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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	Write	group* (p. 1094)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	functions and connectors to perform actions in other AWS services				
AssociateServiceRoleWithAccount	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} (p. 1096)	aws:TagKeys (p. 1096)
CreateConnectorDefinitionVersion	Grants permission to create a version of an existing connector definition	Write	connectorDefinition* (p. 1095)		
CreateCoreDefinition	Grants permission to create a core definition	Write		aws:RequestTag/\${TagKey} (p. 1096)	aws:TagKeys (p. 1096)
CreateCoreDefinitionVersion	Grants permission to create a version of an existing core definition. Greengrass groups must each contain exactly one Greengrass core	Write	coreDefinition* (p. 1094)		
CreateDeployment	Grants permission to create a deployment	Write	group* (p. 1094)		
CreateDeviceDefinition	Grants permission to create a device definition	Write		aws:RequestTag/\${TagKey} (p. 1096)	aws:TagKeys (p. 1096)
CreateDeviceDefinitionVersion	Grants permission to create a version of an existing device definition	Write	deviceDefinition* (p. 1094)		
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} (p. 1096)	aws:TagKeys (p. 1096)
CreateFunctionDefinitionVersion	Grants permission to create a version of an existing Lambda function definition	Write	functionDefinition* (p. 1094)		
CreateGroup	Grants permission to create a group	Write		aws:RequestTag/\${TagKey} (p. 1096)	aws:TagKeys (p. 1096)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateGroupCertificateAuthority for the group, or rotate the existing CA	Grants permission to create a CA for the group, or rotate the existing CA	Write	group* (p. 1094)		
CreateGroupVersion of a group that has already been defined	Grants permission to create a version of a group that has already been defined	Write	group* (p. 1094)		
CreateLoggerDefinition	Grants permission to create a logger definition	Write		aws:RequestTag/\${TagKey} (p. 1096) aws:TagKeys (p. 1096)	
CreateLoggerDefinitionVersion of an existing logger definition	Grants permission to create a version of an existing logger definition	Write	loggerDefinition* (p. 1095)		
CreateResourceDefinition	Grants permission to create a resource definition that contains a list of resources to be used in a group	Write		aws:RequestTag/\${TagKey} (p. 1096) aws:TagKeys (p. 1096)	
CreateResourceDefinitionVersion of an existing resource definition	Grants permission to create a version of an existing resource definition	Write	resourceDefinition* (p. 1095)		
CreateSoftwareUpdateJob	Grants permission to create an AWS S3 job that will trigger your Greengrass cores to update the software they are running	Write			
CreateSubscriptionDefinition	Grants permission to create a subscription definition	Write		aws:RequestTag/\${TagKey} (p. 1096) aws:TagKeys (p. 1096)	
CreateSubscriptionDefinitionVersion of an existing subscription definition	Grants permission to create a version of an existing subscription definition	Write	subscriptionDefinition* (p. 1094)		
DeleteConnectorDefinition	Grants permission to delete a connector definition	Write	connectorDefinition* (p. 1095)		
DeleteCoreDefinition	Grants permission to delete a core definition. Deleting a definition that is currently in use in a deployment affects future deployments	Write	coreDefinition* (p. 1094)		
DeleteDeviceDefinition	Grants permission to delete a device definition. Deleting a definition that is currently in use in a deployment affects future deployments	Write	deviceDefinition* (p. 1094)		

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* (p. 1094)		
DeleteGroup	Grants permission to delete a group that is not currently in use in a deployment	Write	group* (p. 1094)		
DeleteLoggerDefinition	Grants permission to delete a logger definition. Deleting a definition that is currently in use in a deployment affects future deployments	Write	loggerDefinition* (p. 1095)		
DeleteResourceDefinition	Grants permission to delete a resource definition	Write	resourceDefinition* (p. 1095)		
DeleteSubscriptionDefinition	Grants permission to delete a subscription definition. Deleting a definition that is currently in use in a deployment affects future deployments	Write	subscriptionDefinition* (p. 1094)		
DisassociateRoleFromGroup	Grants permission to disassociate the role from a group	Write	group* (p. 1094)		
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* (p. 1095)		
GetAssociatedRole	Grants permission to retrieve the role associated with a group	Read	group* (p. 1094)		
GetBulkDeploymentStatus	Grants permission to return the status of a bulk deployment	Read	bulkDeployment* (p. 1094)		
GetConnectivityInfo	Grants permission to retrieve the connectivity information for a core	Read	connectivityInfo* (p. 1094)		
GetConnectorDefinitionInfo	Grants permission to retrieve information about a connector definition	Read	connectorDefinition* (p. 1095)		
GetConnectorDefinitionVersion		Read	connectorDefinition* (p. 1095)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to retrieve information about a connector definition version		connectorDefinitionVersion* (p. 1095)		
GetCoreDefinition	Grants permission to retrieve information about a core definition	Read	coreDefinition* (p. 1094)		
GetCoreDefinitionInformation	Grants permission to retrieve information about a core definition version	Read	coreDefinition* (p. 1094) coreDefinitionVersion* (p. 1094)		
GetDeploymentStatus	Grants permission to return the status of a deployment	Read	deployment* (p. 1094) group* (p. 1094)		
GetDeviceDefinition	Grants permission to retrieve information about a device definition	Read	deviceDefinition* (p. 1094)		
GetDeviceDefinitionInformation	Grants permission to retrieve information about a device definition version	Read	deviceDefinition* (p. 1094) deviceDefinitionVersion* (p. 1094)		
GetFunctionDefinition	Grants permission to retrieve information about a Lambda function definition, such as its creation time and latest version	Read	functionDefinition* (p. 1094)		
GetFunctionDefinitionInformation	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* (p. 1094) functionDefinitionVersion* (p. 1094)		
GetGroup	Grants permission to retrieve information about a group	Read	group* (p. 1094)		
GetGroupCertificateAuthority	Grants permission to return the public key of the CA associated with a group	Read	certificateAuthority* (p. 1094) group* (p. 1094)		
GetGroupCertificateConfiguration	Grants permission to retrieve the configuration for the CA used by a group	Read	group* (p. 1094)		
GetGroupVersion	Grants permission to retrieve information about a group version	Read	group* (p. 1094) groupVersion* (p. 1094)		
GetLoggerDefinition	Grants permission to retrieve information about a logger definition	Read	loggerDefinition* (p. 1095)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetLoggerDefinition	Grants permission to retrieve information about a logger definition version	Read	loggerDefinition* (p. 1095)		
			loggerDefinitionVersion* (p. 1095)		
GetResourceDefinition	Grants permission to retrieve information about a resource definition, such as its creation time and latest version	Read	resourceDefinition* (p. 1095)		
GetResourceDefinitionInformation	Grants permission to retrieve information about a resource definition version, such as which resources are included in the version	Read	resourceDefinition* (p. 1095)		
			resourceDefinitionVersion* (p. 1095)		
GetServiceRoleForService	Grants permission to retrieve the role that is attached to an account	Read			
GetSubscriptionDefinition	Grants permission to retrieve information about a subscription definition	Read	subscriptionDefinition* (p. 1094)		
GetSubscriptionDefinitionInformation	Grants permission to retrieve information about a subscription definition version	Read	subscriptionDefinition* (p. 1094)		
			subscriptionDefinitionVersion* (p. 1094)		
GetThingRuntimeConfig	Grants permission to retrieve configuration of a thing	Read	thingRuntimeConfig* (p. 1095)		
ListBulkDeployment	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* (p. 1094)		
ListBulkDeploymentList	Grants permission to retrieve a list of bulk deployments	List			
ListConnectorDefinition	Grants permission to list the versions of a connector definition	List	connectorDefinition* (p. 1095)		
ListConnectorDefinitionList	Grants permission to retrieve a list of connector definitions	List			
ListCoreDefinition	Grants permission to list the versions of a core definition	List	coreDefinition* (p. 1094)		
ListCoreDefinitionList	Grants permission to retrieve a list of core definitions	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDeployments	Grants permission to retrieve a list of all deployments for a group	List	group* (p. 1094)		
ListDeviceDefinitionVersions	Grants permission to list the versions of a device definition	List	deviceDefinition* (p. 1094)		
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* (p. 1094)		
ListFunctionDefinitions	Grants permission to retrieve a list of Lambda function definitions	List			
ListGroupCertificates	Grants permission to retrieve a list of current CAs for a group	List	group* (p. 1094)		
ListGroupVersions	Grants permission to list the versions of a group	List	group* (p. 1094)		
ListGroups	Grants permission to retrieve a list of groups	List			
ListLoggerDefinitionVersions	Grants permission to list the versions of a logger definition	List	loggerDefinition* (p. 1095)		
ListLoggerDefinitions	Grants permission to retrieve a list of logger definitions	List			
ListResourceDefinitionVersions	Grants permission to list the versions of a resource definition	List	resourceDefinition* (p. 1095)		
ListResourceDefinitions	Grants permission to retrieve a list of resource definitions	List			
ListSubscriptionDefinitionVersions	Grants permission to list the versions of a subscription definition	List	subscriptionDefinition* (p. 1094)		
ListSubscriptionDefinitions	Grants permission to retrieve a list of subscription definitions	List			
ListTagsForResource	Grants permission to list the tags for a resource	Read	bulkDeployment (p. 1094)		
			connectorDefinition (p. 1095)		
			coreDefinition (p. 1094)		
			deviceDefinition (p. 1094)		
			functionDefinition (p. 1094)		
			group (p. 1094)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			loggerDefinition (p. 1095) resourceDefinition (p. 1095) subscriptionDefinition (p. 1094) aws:RequestTag/\${TagKey} (p. 1096) aws:TagKeys (p. 1096)		
ResetDeployment	Grants permission to reset a group's deployments	Write	group* (p. 1094)		
StartBulkDeployment	Grants permission to deploy multiple groups in one operation	Write	aws:RequestTag/\${TagKey} (p. 1096) aws:TagKeys (p. 1096)		
StopBulkDeployment	Grants permission to stop the execution of a bulk deployment	Write	bulkDeployment* (p. 1094)		
TagResource	Grants permission to add tags to a resource	Tagging	bulkDeployment (p. 1094) connectorDefinition (p. 1095) coreDefinition (p. 1094) deviceDefinition (p. 1094) functionDefinition (p. 1094) group (p. 1094) loggerDefinition (p. 1095) resourceDefinition (p. 1095) subscriptionDefinition (p. 1094) aws:RequestTag/\${TagKey} (p. 1096) aws:TagKeys (p. 1096)		
UntagResource	Grants permission to remove tags from a resource		bulkDeployment (p. 1094) connectorDefinition (p. 1095) coreDefinition (p. 1094) deviceDefinition (p. 1094) functionDefinition (p. 1094) group (p. 1094) loggerDefinition (p. 1095)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			resourceDefinition (p. 1095)		
			subscriptionDefinition (p. 1094)		
			aws:TagKeys (p. 1096)		
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* (p. 1094)		
UpdateConnectorDefinition	Grants permission to update a connector definition	Write	connectorDefinition* (p. 1095)		
UpdateCoreDefinition	Grants permission to update a core definition	Write	coreDefinition* (p. 1094)		
UpdateDeviceDefinition	Grants permission to update a device definition	Write	deviceDefinition* (p. 1094)		
UpdateFunctionDefinition	Grants permission to update a Lambda function definition	Write	functionDefinition* (p. 1094)		
UpdateGroup	Grants permission to update a group	Write	group* (p. 1094)		
UpdateGroupCertificateExpiration	Grants permission to update the certificate expiration time for a group	Write	group* (p. 1094)		
UpdateLoggerDefinition	Grants permission to update a logger definition	Write	loggerDefinition* (p. 1095)		
UpdateResourceDefinition	Grants permission to update a resource definition	Write	resourceDefinition* (p. 1095)		
UpdateSubscriptionDefinition	Grants permission to update a subscription definition	Write	subscriptionDefinition* (p. 1094)		
UpdateThingRuntimeConfiguration	Grants permission to update the runtime configuration of a thing	Write	thingRuntimeConfig* (p. 1095)		

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 \(p. 1085\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1096)
group	arn:\${Partition}:greengrass:\${Region}: \${Account}:/greengrass/groups/\${GroupId}	aws:ResourceTag/\${TagKey} (p. 1096)
groupVersion	arn:\${Partition}:greengrass:\${Region}: \${Account}:/greengrass/groups/\${GroupId}/versions/\${VersionId}	
coreDefinition	arn:\${Partition}:greengrass:\${Region}: \${Account}:/greengrass/definition/cores/\${CoreDefinitionId}	aws:ResourceTag/\${TagKey} (p. 1096)
coreDefinitionVersion	arn:\${Partition}:greengrass:\${Region}: \${Account}:/greengrass/definition/cores/\${CoreDefinitionId}/versions/\${VersionId}	
deviceDefinition	arn:\${Partition}:greengrass:\${Region}: \${Account}:/greengrass/definition/devices/\${DeviceDefinitionId}	aws:ResourceTag/\${TagKey} (p. 1096)
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} (p. 1096)
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} (p. 1096)
subscriptionDefinitionVersion	arn:\${Partition}:greengrass:\${Region}: \${Account}:/greengrass/definition/subscriptions/\${SubscriptionDefinitionId}/versions/\${VersionId}	

Resource types	ARN	Condition keys
	subscriptions/\${SubscriptionDefinitionId}/versions/\${VersionId}	
loggerDefinition	arn:\${Partition}:greengrass:\${Region}:\${Account}:/greengrass/definition/loggers/\${LoggerDefinitionId}	aws:ResourceTag/\${TagKey} (p. 1096)
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} (p. 1096)
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} (p. 1096)
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 [Available global condition keys](#).

Condition keys	Description	Type
aws:CurrentTime	Filters actions based on date/time conditions for the current date and time	Date
aws:EpochTime	Filters actions based on date/time conditions for the current date and time in epoch or Unix time	Date
aws:MultiFactorAuthAge	Filters actions based on how long ago (in seconds) the security credentials validated by multi-factor authentication (MFA) in the request were issued using MFA	Numeric

Condition keys	Description	Type
aws:MultiFactorAuthType	Filters actions based on whether multi-factor authentication (MFA) was used to validate the temporary security credentials that made the current request	Bool
aws:RequestTag/\${TagKey}	Filters actions based on the allowed set of values for each of the mandatory tags	String
aws:ResourceTag/\${TagKey}	Filters actions based on the tag value associated with the resource	String
aws:SecureTransport	Filters actions based on whether the request was sent using SSL	Bool
aws:TagKeys	Filters actions based on the presence of mandatory tags in the request	String
aws:UserAgent	Filters actions based on the requester's client application	String

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 \(p. 1096\)](#)
- [Resource types defined by AWS IoT Greengrass V2 \(p. 1100\)](#)
- [Condition keys for AWS IoT Greengrass V2 \(p. 1101\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateServiceRoleWithYourAccount	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
BatchAssociateClientDevicesWithCoreDevice	Grants permission to associate a list of client devices with a core device	Write	coreDevice* (p. 1101)		
BatchDisassociateClientDevicesFromCoreDevice	Grants permission to disassociate a list of client devices from a core device	Write	coreDevice* (p. 1101)		
CancelDeployment	Grants permission to cancel a deployment	Write	deployment* (p. 1101)		iot:CancelJob iot>DeleteThingShadow iot:DescribeJob iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow iot:UpdateJob iot:UpdateThingShadow
CreateComponent	Grants permission to create a component	Write	component* (p. 1100)		
			aws:RequestTag/\${TagKey} (p. 1101) aws:TagKeys (p. 1101)		
CreateDeployment	Grants permission to create a deployment	Write			aws:RequestJobCancelJob \${TagKey} (p. 1101) iot>CreateJob aws:TagKeys (p. 1101) iot>DeleteThingShadow iot:DescribeJob iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow iot:UpdateJob iot:UpdateThingShadow

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteComponent	Grants permission to delete a component	Write	componentVersion* (p. 1100)		
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* (p. 1101)		iot:DescribeJobExecution
DescribeComponent	Grants permission to retrieve metadata for a version of a component	Read	componentVersion* (p. 1100)		
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* (p. 1100)		
GetComponentVersionSignedURL	Grants permission to get the signed URL to download a public component artifact	Read	componentVersion* (p. 1100)		
GetConnectivityInfo	Grants permission to retrieve the connectivity information for a Greengrass core device	Read	connectivityInfo* (p. 1100)	iot:GetThingShadow	
GetCoreDevice	Grants permission to retrieves metadata for a AWS IoT Greengrass core device	Read	coreDevice* (p. 1101)		
GetDeployment	Grants permission to get a deployment	Read	deployment* (p. 1101)	iot:DescribeJob iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow	
GetServiceRoleForService	Grants permission to retrieve the service role that is attached to an account	Read			
ListClientDevicesAsynchronously	Grants permission to retrieve a paginated list of client devices associated to a AWS IoT Greengrass core device	List	coreDevice* (p. 1101)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListComponentVersions	Grants permission to retrieve a paginated list of all versions for a component	List	component* (p. 1100)		
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
ListEffectiveDeployments	Grants permission to retrieves a paginated list of deployment jobs that AWS IoT Greengrass sends to AWS IoT Greengrass core devices	List	coreDevice* (p. 1101)		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* (p. 1101)		
ListTagsForResource	Grants permission to list the tags for a resource	Read	component (p. 1100)		
			componentVersion (p. 1100)		
			coreDevice (p. 1101)		
			deployment (p. 1101)		
			aws:RequestTag/\${TagKey} (p. 1101)		
			aws:TagKeys (p. 1101)		
ResolveComponents	Grants permission to list components that meet the component, version, and platform requirements of a deployment	List	componentVersion* (p. 1100)		
TagResource	Grants permission to add tags to a resource	Tagging	component (p. 1100)		
			componentVersion (p. 1100)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			coreDevice (p. 1101) deployment (p. 1101) aws:RequestTag/\${TagKey} (p. 1101) aws:TagKeys (p. 1101)		
UntagResource	Grants permission to remove tags from a resource	Tagging	component (p. 1100) componentVersion (p. 1100) coreDevice (p. 1101) deployment (p. 1101) aws:RequestTag/\${TagKey} (p. 1101) aws:TagKeys (p. 1101)		
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* (p. 1100)	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 \(p. 1096\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1101)
componentVersion	arn:\${Partition}:greengrass:\${Region}:\${Account}:components:\${ComponentName}:versions:\${ComponentVersion}	aws:ResourceTag/\${TagKey} (p. 1101)

Resource types	ARN	Condition keys
coreDevice	arn:\${Partition}:greengrass:\${Region}:\${Account}:coreDevices:\${CoreDeviceThingName}	aws:ResourceTag/\${TagKey} (p. 1101)
deployment	arn:\${Partition}:greengrass:\${Region}:\${Account}:deployments:\${DeploymentId}	aws:ResourceTag/\${TagKey} (p. 1101)

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 [Available global condition keys](#).

Condition keys	Description	Type
aws:CurrentTime	Filters access by checking date/time conditions for the current date and time	Date
aws:EpochTime	Filters access by checking date/time conditions for the current date and time in epoch or Unix time	Date
aws:MultiFactorAuthAge	Filters access by checking how long ago (in seconds) the security credentials validated by multi-factor authentication (MFA) in the request were issued using MFA	Numeric
aws:MultiFactorAuthPendingAuthentication	Filters access by checking whether multi-factor authentication (MFA) was used to validate the temporary security credentials that made the current request	Bool
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:SecureTransport	Filters access by checking whether the request was sent using SSL	Bool
aws:TagKeys	Filters access by checking tag keys passed in the request	ArrayOfString
aws:UserAgent	Filters access by the requester's client application	String

Actions, resources, and condition keys for AWS IoT Jobs DataPlane

AWS IoT Jobs DataPlane (service prefix: iot-jobsdata) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to [configure this service](#).
- View a list of the [API 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 \(p. 1102\)](#)
- [Resource types defined by AWS IoT Jobs DataPlane \(p. 1102\)](#)
- [Condition keys for AWS IoT Jobs DataPlane \(p. 1103\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1103)		
			iot:JobId (p. 1103)		
GetPendingJobExecution	Grants permission to get the list of pending jobs for a thing that are not in a terminal state	Read	thing* (p. 1103)		
StartNextPendingJobExecution	Grants permission to get and start the next pending job execution for a thing	Write	thing* (p. 1103)		
UpdateJobExecution	Grants permission to update a job execution	Write	thing* (p. 1103)		
			iot:JobId (p. 1103)		

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 \(p. 1102\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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 [Available global condition keys](#).

Condition keys	Description	Type
iot:JobId	Filters access by jobId for <code>iotjobsdata:DescribeJobExecution</code> and <code>iotjobsdata:UpdateJobExecution</code> APIs	String

Actions, resources, and condition keys for AWS IoT RoboRunner

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

References:

- Learn how to [configure this service](#).
- View a list of the [API 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 RoboRunner \(p. 1103\)](#)
- [Resource types defined by AWS IoT RoboRunner \(p. 1106\)](#)
- [Condition keys for AWS IoT RoboRunner \(p. 1107\)](#)

Actions defined by AWS IoT RoboRunner

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

The **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAction	Grants permission to create an action	Write			
CreateActionTemplate	Grants permission to create an action template	Write			
CreateActionTemplateDependency	Grants permission to create an action template dependency	Write			
CreateActivity	Grants permission to create an activity	Write			
CreateActivityDependency	Grants permission to create an activity dependency	Write			
CreateDestination	Grants permission to create a destination	Write			
CreateDestinationRelationship	Grants permission to create a destination relationship	Write			
CreateSite	Grants permission to create a site	Write			
CreateTask	Grants permission to create a task	Write			
CreateTaskDependency	Grants permission to create a task dependency	Write			
CreateWorker	Grants permission to create a worker	Write			
CreateWorkerFleet	Grants permission to create a worker fleet	Write			
DeleteAction	Grants permission to delete an action	Write	ActionResource* (p. 1106)		
DeleteActionTemplate	Grants permission to delete an action template	Write	ActionTemplateResource* (p. 1106)		
DeleteActionTemplateDependency	Grants permission to delete an action template dependency	Write			
DeleteActivity	Grants permission to delete an activity	Write	ActivityResource* (p. 1106)		
DeleteActivityDependency	Grants permission to delete an activity dependency	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteDestination	Grants permission to delete a destination	Write	DestinationResource* (p. 1107)		
DeleteDestinationRelationship	Grants permission to delete a destination relationship	Write	DestinationRelationshipResource* (p. 1107)		
DeleteSite	Grants permission to delete a site	Write	SiteResource* (p. 1107)		
DeleteTask	Grants permission to delete a task	Write	TaskResource* (p. 1107)		
DeleteTaskDependency	Grants permission to delete a task dependency	Write			
DeleteWorker	Grants permission to delete a worker	Write	WorkerResource* (p. 1107)		
DeleteWorkerFleet	Grants permission to delete a worker fleet	Write	WorkerFleetResource* (p. 1107)		
GetAction	Grants permission to get an action	Read	ActionResource* (p. 1106)		
GetActionTemplate	Grants permission to get an action template	Read	ActionTemplateResource* (p. 1106)		
GetActivity	Grants permission to get an activity	Read	ActivityResource* (p. 1106)		
GetDestination	Grants permission to get a destination	Read	DestinationResource* (p. 1107)		
GetDestinationRelationship	Grants permission to get a destination relationship	Read	DestinationRelationshipResource* (p. 1107)		
GetSite	Grants permission to get a site	Read	SiteResource* (p. 1107)		
GetTask	Grants permission to get a task	Read	TaskResource* (p. 1107)		
GetWorker	Grants permission to get a worker	Read	WorkerResource* (p. 1107)		
GetWorkerFleet	Grants permission to get a worker fleet	Read	WorkerFleetResource* (p. 1107)		
ListActionTemplates	Grants permission to list action templates	Read			
ListActions	Grants permission to list actions	Read			
ListActivities	Grants permission to list activities	Read			
ListDestinationRelationships	Grants permission to list destination relationships	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDestinations	Grants permission to list destinations	Read			
ListSites	Grants permission to list sites	Read			
ListTasks	Grants permission to list tasks	Read			
ListWorkerFleets	Grants permission to list worker fleets	Read			
ListWorkers	Grants permission to list workers	Read			
UpdateActionState	Grants permission to update an action's state	Write	ActionResource* (p. 1106)		
UpdateActivity	Grants permission to update an activity	Write	ActivityResource* (p. 1106)		
UpdateDestination	Grants permission to update a destination	Write	DestinationResource* (p. 1107)		
UpdateSite	Grants permission to update a site	Write	SiteResource* (p. 1107)		
UpdateTask	Grants permission to update a task	Write	TaskResource* (p. 1107)		
UpdateWorker	Grants permission to update a worker	Write	WorkerResource* (p. 1107)		
UpdateWorkerFleet	Grants permission to update a worker fleet	Write	WorkerFleetResource* (p. 1107)		

Resource types defined by AWS IoT RoboRunner

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the [Actions table \(p. 1103\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
ActionResource	<code>arn:\${Partition}:iotroborunner:\${Region}: \${Account}:action/\${ActionId}</code>	iotroborunner:ActionResourceId (p. 1106)
ActionTemplateResource	<code>arn:\${Partition}:iotroborunner: \${Region}: \${Account}:action-template/ \${ActionTemplateId}</code>	iotroborunner:ActionTemplateResource (p. 1106)
ActivityResource	<code>arn:\${Partition}:iotroborunner:\${Region}: \${Account}:activity/\${ActivityId}</code>	iotroborunner:ActivityResourceId (p. 1106)

Resource types	ARN	Condition keys
DestinationRelationship	arn:\${Partition}:iotroborunner:\${Region}: \${Account}:destination-relationship/\${DestinationRelationshipId}	iotroborunner:DestinationRelationshipId
DestinationResource	arn:\${Partition}:iotroborunner:\${Region}: \${Account}:destination/\${DestinationId}	iotroborunner:DestinationResourceId
SiteResource	arn:\${Partition}:iotroborunner:\${Region}: \${Account}:site/\${SiteId}	iotroborunner:SiteResourceId (p. 1107)
TaggingResource	arn:\${Partition}:iotroborunner:\${Region}: \${Account}:tag/\${TagKey}	iotroborunner:TaggingResourceTagKey
TaskResource	arn:\${Partition}:iotroborunner:\${Region}: \${Account}:task/\${TaskId}	iotroborunner:TaskResourceId (p. 1107)
WorkerFleetResource	arn:\${Partition}:iotroborunner:\${Region}: \${Account}:worker-fleet/\${WorkerFleetId}	iotroborunner:WorkerFleetResourceId
WorkerResource	arn:\${Partition}:iotroborunner:\${Region}: \${Account}:worker/\${WorkerId}	iotroborunner:WorkerResourceId (p. 1107)

Condition keys for AWS IoT RoboRunner

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

To view the global condition keys that are available to all services, see [Available global condition keys](#).

Condition keys	Description	Type
iotroborunner:ActionResourceId	Filters access by the action's identifier	String
iotroborunner:ActionTemplateResourceId	Filters access by the action template's identifier	String
iotroborunner:ActivityResourceId	Filters access by the activity's identifier	String
iotroborunner:DestinationRelationshipResourceId	Filters access by the destination relationship's identifier	String
iotroborunner:DestinationResourceId	Filters access by the destination's identifier	String
iotroborunner:SiteResourceId	Filters access by the site's identifier	String
iotroborunner:TaggingResourceTagKey	Filters access by the metadata tag name	String
iotroborunner:TaskResourceId	Filters access by the task's identifier	String

Condition keys	Description	Type
iotroborunner:WorkerFleetResourceId	Filters access by the worker fleet's identifier	String
iotroborunner:WorkerResourceId	Filters access by the workers identifier	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 \(p. 1108\)](#)
- [Resource types defined by AWS IoT SiteWise \(p. 1114\)](#)
- [Condition keys for AWS IoT SiteWise \(p. 1115\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1114)		
AssociateTimeSeriesToAssetProperty		Write	asset* (p. 1114)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to associate a time series with an asset property		time-series* (p. 1114)		
BatchAssociateProjectAssets	Grants permission to associate assets to a project	Write	project* (p. 1115)		
BatchDisassociateAssets	Grants permission to dissociate assets from a project	Write	project* (p. 1115)		
BatchGetAssetProperties	Grants permission to retrieve computed aggregates for multiple asset properties	Read	asset (p. 1114)		
			time-series (p. 1114)		
BatchGetAssetPropertyValues	Grants permission to retrieve the latest value for multiple asset properties	Read	asset (p. 1114)		
			time-series (p. 1114)		
BatchPutAssetPropertyValue	Grants permission to put property values for asset properties	Write	asset (p. 1114)		
			time-series (p. 1114)		
CreateAccessPolicy	Grants permission to create an access policy for a portal or a project	Write	portal (p. 1115)		
			project (p. 1115)		
			aws:RequestTag/\${TagKey} (p. 1115)		
CreateAsset	Grants permission to create an asset from an asset model	Write	asset-model* (p. 1114)		
			aws:RequestTag/\${TagKey} (p. 1115)		aws:TagKeys (p. 1115)
CreateAssetModel	Grants permission to create an asset model	Write	aws:RequestTag/\${TagKey} (p. 1115)		aws:TagKeys (p. 1115)
CreateDashboard	Grants permission to create a dashboard in a project	Write	project* (p. 1115)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 1115) aws:TagKeys (p. 1115)	
CreateGateway	Grants permission to create a gateway	Write		aws:RequestTag/ \${TagKey} (p. 1115) aws:TagKeys (p. 1115)	
CreatePortal	Grants permission to create a portal	Write		aws:RequestTag/ \${TagKey} (p. 1115) aws:TagKeys (p. 1115)	sso:CreateManagedApplication (p. 1115) sso:DescribeRegisteredResource (p. 1115)
CreateProject	Grants permission to create a project in a portal	Write		portal* (p. 1115) aws:RequestTag/ \${TagKey} (p. 1115) aws:TagKeys (p. 1115)	
DeleteAccessPolicy	Grants permission to delete an access policy	Write	access-policy* (p. 1115)		
DeleteAsset	Grants permission to delete an asset	Write	asset* (p. 1114)		
DeleteAssetModel	Grants permission to delete an asset model	Write	asset-model* (p. 1114)		
DeleteDashboard	Grants permission to delete a dashboard	Write	dashboard* (p. 1115)		
DeleteGateway	Grants permission to delete a gateway	Write	gateway* (p. 1114)		
DeletePortal	Grants permission to delete a portal	Write	portal* (p. 1115)		sso:DeleteManagedApplication (p. 1115)
DeleteProject	Grants permission to delete a project	Write	project* (p. 1115)		
DeleteTimeSeries	Grants permission to delete a time series	Write	asset (p. 1114) time-series (p. 1114)		
DescribeAccessPolicy	Grants permission to describe an access policy	Read	access-policy* (p. 1115)		
DescribeAsset	Grants permission to describe an asset	Read	asset* (p. 1114)		
DescribeAssetModel	Grants permission to describe an asset model	Read	asset-model* (p. 1114)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeAssetProperties	Grants permission to describe an asset property	Read	asset* (p. 1114)		
DescribeDashboard	Grants permission to describe a dashboard	Read	dashboard* (p. 1115)		
DescribeDefaultEncryption	Grants permission to describe the default encryption configuration for the AWS account	Read			
DescribeGateway	Grants permission to describe a gateway	Read	gateway* (p. 1114)		
DescribeGatewayCapabilityConfiguration	Grants permission to describe capability configuration for a gateway	Read	gateway* (p. 1114)		
DescribeLogging	Grants permission to describe logging options for the AWS account	Read			
DescribePortal	Grants permission to describe a portal	Read	portal* (p. 1115)		
DescribeProject	Grants permission to describe a project	Read	project* (p. 1115)		
DescribeStorageConfiguration	Grants permission to describe the storage configuration for the AWS account	Read			
DescribeTimeSeries	Grants permission to describe a time series	Read	asset (p. 1114) time-series (p. 1114)		
DisassociateAsset	Grants permission to disassociate a child asset from a parent asset by a hierarchy	Write	asset* (p. 1114)		
DisassociateTimeSeries	Grants permission to disassociate a time series from an asset property	Write	asset* (p. 1114) time-series* (p. 1114)		
GetAssetPropertyComputedAggregates	Grants permission to retrieve computed aggregates for an asset property	Read	asset (p. 1114) time-series (p. 1114)		
GetAssetPropertyLatestValue	Grants permission to retrieve the latest value for an asset property	Read	asset (p. 1114) time-series (p. 1114)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAssetProperty	Grants permission to retrieve the value history for an asset property	Read	asset (p. 1114)		
			time-series (p. 1114)		
GetInterpolatedAssetValues	Grants permission to retrieve interpolated values for an asset property	Read	asset (p. 1114)		
			time-series (p. 1114)		
ListAccessPolicies	Grants permission to list all access policies for an identity or a resource	List	portal (p. 1115)		
			project (p. 1115)		
ListAssetModels	Grants permission to list all asset models	List			
ListAssetRelationships	Grants permission to list the asset relationship graph for an asset	List	asset* (p. 1114)		
ListAssets	Grants permission to list all assets	List	asset-model (p. 1114)		
ListAssociatedAssets	Grants permission to list all assets associated with an asset through a hierarchy	List	asset* (p. 1114)		
ListDashboards	Grants permission to list all dashboards in a project	List	project* (p. 1115)		
ListGateways	Grants permission to list all gateways	List			
ListPortals	Grants permission to list all portals	List			
ListProjectAssets	Grants permission to list all assets associated with a project	List	project* (p. 1115)		
ListProjects	Grants permission to list all projects in a portal	List	portal* (p. 1115)		
ListTagsForResource	Grants permission to list all tags for a resource	Read	access-policy (p. 1115)		
			asset (p. 1114)		
			asset-model (p. 1114)		
			dashboard (p. 1115)		
			gateway (p. 1114)		
			portal (p. 1115)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			project (p. 1115)		
			aws:ResourceTag/ \${TagKey} (p. 1115)		
ListTimeSeries	Grants permission to list time series	List	asset (p. 1114)		
PutDefaultEncryptionConfiguration	Grants permission to set the <code>defaultEncryptionConfiguration</code> 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 (p. 1115)		
asset (p. 1114)					
asset-model (p. 1114)					
dashboard (p. 1115)					
gateway (p. 1114)					
portal (p. 1115)					
project (p. 1115)					
aws:TagKeys (p. 1115)					
UntagResource	Grants permission to untag a resource	Tagging	access-policy (p. 1115)		
asset (p. 1114)					
asset-model (p. 1114)					
dashboard (p. 1115)					
gateway (p. 1114)					
portal (p. 1115)					
project (p. 1115)					
aws:TagKeys (p. 1115)					

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAccessPolicy	Grants permission to update an access policy	Write	access-policy* (p. 1115)		
UpdateAsset	Grants permission to update an asset	Write	asset* (p. 1114)		
UpdateAssetModel	Grants permission to update an asset model	Write	asset-model* (p. 1114)		
UpdateAssetModelProperty	Grants permission to update an Asset Model property routing	Write	asset-model* (p. 1114)		
UpdateAssetProperty	Grants permission to update an asset property	Write	asset* (p. 1114)		
UpdateDashboard	Grants permission to update a dashboard	Write	dashboard* (p. 1115)		
UpdateGateway	Grants permission to update a gateway	Write	gateway* (p. 1114)		
UpdateGatewayCapabilityConfiguration	Grants permission to update a gateway capability configuration for a gateway	Write	gateway* (p. 1114)		
UpdatePortal	Grants permission to update a portal	Write	portal* (p. 1115)		
UpdateProject	Grants permission to update a project	Write	project* (p. 1115)		

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 \(p. 1108\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
asset	<code>arn:\${Partition}:iotsitewise:\${Region}: \${Account}:asset/\${AssetId}</code>	aws:ResourceTag/\${TagKey} (p. 1115)
asset-model	<code>arn:\${Partition}:iotsitewise:\${Region}: \${Account}:asset-model/\${AssetModelId}</code>	aws:ResourceTag/\${TagKey} (p. 1115)
time-series	<code>arn:\${Partition}:iotsitewise:\${Region}: \${Account}:time-series/\${TimeSeriesId}</code>	
gateway	<code>arn:\${Partition}:iotsitewise:\${Region}: \${Account}:gateway/\${GatewayId}</code>	aws:ResourceTag/\${TagKey} (p. 1115)

Resource types	ARN	Condition keys
portal	arn:\${Partition}:iotsitewise:\${Region}: \${Account}:portal/\${PortalId}	aws:ResourceTag/ \${TagKey} (p. 1115)
project	arn:\${Partition}:iotsitewise:\${Region}: \${Account}:project/\${ProjectId}	aws:ResourceTag/ \${TagKey} (p. 1115)
dashboard	arn:\${Partition}:iotsitewise:\${Region}: \${Account}:dashboard/\${DashboardId}	aws:ResourceTag/ \${TagKey} (p. 1115)
access-policy	arn:\${Partition}:iotsitewise:\${Region}: \${Account}:access-policy/\${AccessPolicyId}	aws:ResourceTag/ \${TagKey} (p. 1115)

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 [Available global condition 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
iotsitewise:assetHierarchyIds	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 with 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:isAssociatedWithAsset	Filters access by data streams associated with or not associated with an 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 Things Graph

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

References:

- Learn how to [configure this service](#).
- View a list of the [API 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 Things Graph \(p. 1116\)](#)
- [Resource types defined by AWS IoT Things Graph \(p. 1120\)](#)
- [Condition keys for AWS IoT Things Graph \(p. 1121\)](#)

Actions defined by AWS IoT Things Graph

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

The **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateEntityToThing	Associates a device with a concrete thing that is in the user's registry. A thing can be associated with only one device at a time. If you associate a thing with a new device id, its previous association will be removed	Write			iot:DescribeThing iot:DescribeThingGroup
CreateFlowTemplate	Creates a workflow template. Workflows can be created only in the user's namespace. (The public namespace contains only entities.) The workflow can contain only entities in	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	the specified namespace. The workflow is validated against the entities in the latest version of the user's namespace unless another namespace version is specified in the request				
CreateSystemInstance	Creates an instance of a system with specified configurations and Things	Write		aws:RequestTag/\${TagKey} (p. 1121)	aws:TagKeys (p. 1121)
CreateSystemTemplate	Creates a system. The system is validated against the entities in the latest version of the user's namespace unless another namespace version is specified in the request	Write			
DeleteFlowTemplate	Deletes a workflow. Any new system or system instance that contains this workflow will fail to update or deploy. Existing system instances that contain the workflow will continue to run (since they use a snapshot of the workflow taken at the time of deploying the system instance)	Write	Workflow* (p. 1120)		
DeleteNamespace	Deletes the specified namespace. This action deletes all of the entities in the namespace. Delete the systems and flows in the namespace before performing this action	Write			
DeleteSystemInstance	Deletes a system instance. Only instances that have never been deployed, or that have been undeployed from the target can be deleted. Users can create a new system instance that has the same ID as a deleted system instance	Write	SystemInstance* (p. 1120)		
DeleteSystemTemplate	Deletes a system. New system instances can't contain the system after its deletion. Existing system instances that contain the system will continue to work because they use a snapshot of the system that is taken when it is deployed	Write	System* (p. 1120)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeploySystemInstance	Deploys the system instance to the target specified in CreateSystemInstance	Write	SystemInstance* (p. 1120)		
DeprecateFlowTemplate	Deprecates the specified workflow. This action marks the workflow for deletion. Deprecated flows can't be deployed, but existing system instances that use the flow will continue to run	Write	Workflow* (p. 1120)		
DeprecateSystemTemplate	Deprecates the specified system template	Write	System* (p. 1120)		
DescribeNamespace	Gets the latest version of the user's namespace and the public version that it is tracking	Read			
DissociateEntityFromThing	Dissociates a device entity from a thing. The action takes only the type of the entity that you need to dissociate because only one entity of a particular type can be associated with a thing	Write			iot:DescribeThing iot:DescribeThingGroup
GetEntities	Gets descriptions of the specified entities. Uses the latest version of the user's namespace by default	Read			
GetFlowTemplate	Gets the latest version of the DefinitionDocument and FlowTemplateSummary for the specified workflow	Read	Workflow* (p. 1120)		
GetFlowTemplateHistory	Gets revisions of the specified workflow. Only the last 100 revisions are stored. If the workflow has been deprecated, this action will return revisions that occurred before the deprecation. This action won't work for workflows that have been deleted	Read	Workflow* (p. 1120)		
GetNamespaceDeletionStatus	Gets the status of a namespace deletion task	Read			
GetSystemInstance	Gets a system instance	Read	SystemInstance* (p. 1120)		
GetSystemTemplate	Gets a system template	Read	System* (p. 1120)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSystemTemplateRevisions	Gets revisions made to the specified system template. Only the previous 100 revisions are stored. If the system has been deprecated, this action will return the revisions that occurred before its deprecation. This action won't work with systems that have been deleted	Read	System* (p. 1120)		
GetUploadStatus	Gets the status of the specified upload	Read			
ListFlowExecutionDetails	Lists details of a single workflow execution	List			
ListTagsForResource	Lists all tags for a given resource	List	SystemInstance (p. 1120)		
SearchEntities	Searches for entities of the specified type. You can search for entities in your namespace and the public namespace that you're tracking	Read			
SearchFlowExecutionDetails	Searches for workflow executions of a system instance	Read	SystemInstance* (p. 1120)		
SearchFlowTemplateInfo	Searches for summary information about workflows	Read			
SearchSystemInstances	Searches for system instances in the user's account	Read			
SearchSystemTemplateInfo	Searches for summary information about systems in the user's account. You can filter by the ID of a workflow to return only systems that use the specified workflow	Read			
SearchThings	Searches for things associated with the specified entity. You can search by both device and device model	Read			
TagResource	Tag a specified resource	Tagging	SystemInstance (p. 1120)		
				aws:RequestTag/\${TagKey} (p. 1121)	
					aws:TagKeys (p. 1121)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UndeploySystemInstance	Removes the system instance and associated triggers from the target	Write	SystemInstance* (p. 1120)		
UntagResource	Untag a specified resource	Tagging	SystemInstance (p. 1120)		
				aws:TagKeys (p. 1121)	
UpdateFlowTemplate	Updates the specified workflow. All deployed systems and system instances that use the workflow will see the changes in the flow when it is redeployed. The workflow can contain only entities in the specified namespace	Write	Workflow* (p. 1120)		
UpdateSystemTemplate	Updates the specified system. You don't need to run this action after updating a workflow. Any system instance that uses the system will see the changes in the system when it is redeployed	Write	System* (p. 1120)		
UploadEntityDefinitions	Asynchronously uploads one or more entity definitions to the user's namespace	Write			

Resource types defined by AWS IoT Things Graph

The following resource types are defined by this service and can be used in the Resource element of IAM permission policy statements. Each action in the [Actions table \(p. 1116\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
Workflow	arn:\${Partition}:iotthingsgraph:\${Region}:\${Account}:Workflow/\${NamespacePath}	
System	arn:\${Partition}:iotthingsgraph:\${Region}:\${Account}:System/\${NamespacePath}	
SystemInstance	arn:\${Partition}:iotthingsgraph:\${Region}:\${Account}:Deployment/\${NamespacePath}	aws:ResourceTag/\${TagKey} (p. 1121)

Condition keys for AWS IoT Things Graph

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

To view the global condition keys that are available to all services, see [Available global condition keys](#).

Condition keys	Description	Type
aws:RequestTag/\${TagKey}	Filters access by a key that is present in the request the user makes to the thingsgraph 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 thingsgraph service	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 \(p. 1121\)](#)
- [Resource types defined by AWS IoT TwinMaker \(p. 1124\)](#)
- [Condition keys for AWS IoT TwinMaker \(p. 1125\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1124)		iottwinmaker:GetComponentType
			entity (p. 1124)		iottwinmaker:GetEntity
CreateComponentType	Grants permission to create a component type	Write	workspace* (p. 1124)		iottwinmaker:GetWorkspace
			aws:RequestTag/ \${TagKey} (p. 1125)		
CreateEntity	Grants permission to create an entity	Write	aws:RequestTag/ \${TagKey} (p. 1125)		
			aws:TagKeys (p. 1125)		
CreateScene	Grants permission to create a scene	Write	aws:RequestTag/ \${TagKey} (p. 1125)		
			aws:TagKeys (p. 1125)		
CreateWorkspace	Grants permission to create a workspace	Write	aws:RequestTag/ \${TagKey} (p. 1125)		
			aws:TagKeys (p. 1125)		
DeleteComponentType	Grants permission to delete a component type	Write	componentType* (p. 1124)		
			workspace* (p. 1124)		
DeleteEntity	Grants permission to delete an entity	Write	entity* (p. 1124)		
			workspace* (p. 1124)		
DeleteScene	Grants permission to delete a scene	Write	scene* (p. 1125)		
			workspace* (p. 1124)		
DeleteWorkspace	Grants permission to delete a workspace	Write	workspace* (p. 1124)		
GetComponentType	Grants permission to get a component type	Read	componentType* (p. 1124)		
			workspace* (p. 1124)		
GetEntity	Grants permission to get an entity	Read	entity* (p. 1124)		
			workspace* (p. 1124)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetPropertyValues	Grants permission to retrieve the property values	Read	workspace* (p. 1124)		iotwinmaker:GetComponent iotwinmaker:GetEntity iotwinmaker:GetWorkspace
			componentType (p. 1124)		
			entity (p. 1124)		
GetPropertyValuesForTimeSeries	Grants permission to retrieve the time series value history	Read	workspace* (p. 1124)		iotwinmaker:GetComponent iotwinmaker:GetEntity iotwinmaker:GetWorkspace
			componentType (p. 1124)		
			entity (p. 1124)		
GetScene	Grants permission to get a scene	Read	scene* (p. 1125)		
GetWorkspace	Grants permission to get a workspace	Read	workspace* (p. 1124)		
ListComponentTypes	Grants permission to list all componentTypes in a workspace	List	workspace* (p. 1124)		
ListEntities	Grants permission to list all entities in a workspace	List	workspace* (p. 1124)		
ListScenes	Grants permission to list all scenes in a workspace	List	workspace* (p. 1124)		
ListTagsForResource	Grants permission to list all tags for a resource	List	componentType (p. 1124)		
entity (p. 1124)					
scene (p. 1125)					
workspace (p. 1124)					
aws:ResourceTag/ {\$TagKey} (p. 1125)					
ListWorkspaces	Grants permission to list all workspaces	List			
TagResource	Grants permission to tag a resource	Tagging	componentType (p. 1124)		
entity (p. 1124)					
scene (p. 1125)					
workspace (p. 1124)					

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 1125) aws:TagKeys (p. 1125)	
UntagResource	Grants permission to untag a resource	Tagging	componentType (p. 1124)		
			entity (p. 1124)		
			scene (p. 1125)		
			workspace (p. 1124)		
				aws:TagKeys (p. 1125)	
UpdateComponentType	Grants permission to update a componentType	Write	componentType* (p. 1124)		
			workspace* (p. 1124)		
UpdateEntity	Grants permission to update an entity	Write	entity* (p. 1124)		
			workspace* (p. 1124)		
UpdateScene	Grants permission to update a scene	Write	scene* (p. 1125)		
			workspace* (p. 1124)		
UpdateWorkspace	Grants permission to update a workspace	Write	workspace* (p. 1124)		

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 \(p. 1121\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1125)
entity	arn:\${Partition}:iottwinmaker:\${Region}: \${Account}:workspace/\${WorkspaceId}/entity/ \${EntityId}	aws:ResourceTag/ \${TagKey} (p. 1125)
componentType	arn:\${Partition}:iottwinmaker:\${Region}: \${Account}:workspace/\${WorkspaceId}/ component-type/\${ComponentTypeId}	aws:ResourceTag/ \${TagKey} (p. 1125)

Resource types	ARN	Condition keys
scene	arn:\${Partition}:iottwinmaker:\${Region}:\${Account}:workspace/\${WorkspaceId}/scene/\${SceneId}	aws:ResourceTag/\${TagKey} (p. 1125)

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 [Available global condition 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	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 \(p. 1125\)](#)
- [Resource types defined by AWS IQ \(p. 1126\)](#)
- [Condition keys for AWS IQ \(p. 1126\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in

a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateProject [permission only]	Grants permission to submit new project requests	Write			

Resource types defined by AWS IQ

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

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 [Available keys for conditions](#).

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 \(p. 1126\)](#)
- [Resource types defined by AWS IQ Permissions \(p. 1127\)](#)
- [Condition keys for AWS IQ Permissions \(p. 1127\)](#)

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

policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ApproveAccessGrant [permission only]	Grants permission to approve an access grant	Write			

Resource types defined by AWS IQ Permissions

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

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 [Available keys for conditions](#).

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 \(p. 1127\)](#)
- [Resource types defined by Amazon Kendra \(p. 1133\)](#)
- [Condition keys for Amazon Kendra \(p. 1133\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateEntitiesToIndex	Grants permission to put principal mapping in index	Write	experience* (p. 1133)		
			index* (p. 1133)		
AssociatePersonasToEntities	Defines the specific permissions of <code>Entities</code> groups in your AWS SSO identity source with access to your Amazon Kendra experience	Write	experience* (p. 1133)		
			index* (p. 1133)		
BatchDeleteDocuments	Grants permission to batch delete document	Write	index* (p. 1133)		
BatchGetDocumentStatus	Grants permission to do batch get document status	Read	index* (p. 1133)		
BatchPutDocuments	Grants permission to batch put document	Write	index* (p. 1133)		
ClearQuerySuggestions	Grants permission to clear out the suggestions for a given index, generated so far	Write	index* (p. 1133)		
CreateDataSource	Grants permission to create a data source	Write	index* (p. 1133)		
			aws:RequestTag/ \${TagKey} (p. 1134) aws:TagKeys (p. 1134)		
CreateExperience	Creates an Amazon Kendra experience such as a search application	Write	index* (p. 1133)		
CreateFaq	Grants permission to create an Faq	Write	index* (p. 1133)		
			aws:RequestTag/ \${TagKey} (p. 1134) aws:TagKeys (p. 1134)		
CreateIndex	Grants permission to create an Index	Write		aws:RequestTag/ \${TagKey} (p. 1134)	

Service Authorization Reference
Service Authorization Reference
Amazon Kendra

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys (p. 1134)	
CreateQuerySuggestionsBlockList	Grants permission to create a Query Suggestions BlockList	Write	index* (p. 1133) aws:RequestTag/ \${TagKey} (p. 1134) aws:TagKeys (p. 1134)		
CreateThesaurus	Grants permission to create a Thesaurus	Write	index* (p. 1133) aws:RequestTag/ \${TagKey} (p. 1134) aws:TagKeys (p. 1134)		
DeleteDataSource	Grants permission to delete a data source	Write	data-source* (p. 1133) index* (p. 1133)		
DeleteExperience	Deletes your Amazon Kendra experience such as a search application	Write	experience* (p. 1133) index* (p. 1133)		
DeleteFaq	Grants permission to delete an Faq	Write	faq* (p. 1133) index* (p. 1133)		
DeleteIndex	Grants permission to delete an Index	Write	index* (p. 1133)		
DeletePrincipalMapping	Grants permission to delete a principal mapping from index	Write	index* (p. 1133) data-source (p. 1133)		
DeleteQuerySuggestionsBlockList	Grants permission to delete a Query Suggestions BlockList	Write	index* (p. 1133) query-suggestions-block-list* (p. 1133)		
DeleteThesaurus	Grants permission to delete a Thesaurus	Write	index* (p. 1133) thesaurus* (p. 1133)		
DescribeDataSource	Grants permission to describe a data source	Read	data-source* (p. 1133) index* (p. 1133)		
DescribeExperience	Gets information about your Amazon Kendra experience such as a search application	Read	experience* (p. 1133) index* (p. 1133)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeFaq	Grants permission to describe an Faq	Read	faq* (p. 1133)		
			index* (p. 1133)		
DescribeIndex	Grants permission to describe an Index	Read	index* (p. 1133)		
DescribePrincipalMapping	Grants permission to describe Principal mapping from index	Read	index* (p. 1133)		
			data-source (p. 1133)		
DescribeQuerySuggestionsBlockList	Grants permission to describe a QuerySuggestions BlockList	Read	index* (p. 1133)		
			query-suggestions-block-list* (p. 1133)		
DescribeQuerySuggestionsConfiguration	Grants permission to describe the query suggestions configuration for an index	Read	index* (p. 1133)		
DescribeThesaurus	Grants permission to describe a Thesaurus	Read	index* (p. 1133)		
			thesaurus* (p. 1133)		
DisassociateEntityFromAWSIdentity	Prevents users or groups in your AWS SSO identity source from accessing your Amazon Kendra experience	Write	experience* (p. 1133)		
			index* (p. 1133)		
DisassociatePermissionsFromEntity	Removes the specific permissions of users or groups in your AWS SSO identity source with access to your Amazon Kendra experience	Write	experience* (p. 1133)		
			index* (p. 1133)		
GetQuerySuggestions	Grants permission to get Suggestions for a query prefix	Read	index* (p. 1133)		
GetSnapshots	Retrieves search metrics data	Read	index* (p. 1133)		
ListDataSourceSyncJobHistory	Grants permission to get Data Source sync job history	List	data-source* (p. 1133)		
			index* (p. 1133)		
ListDataSources	Grants permission to list the data sources	List	index* (p. 1133)		
ListEntityPermissions	Lists specific permissions of users and groups with access to your Amazon Kendra experience	List	experience* (p. 1133)		
			index* (p. 1133)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListExperienceEntries	Lists users or groups in your AWS SSO identity source that are granted access to your Amazon Kendra experience	List	experience* (p. 1133)		
			index* (p. 1133)		
ListExperiences	Lists one or more Amazon Kendra experiences. You can create an Amazon Kendra experience such as a search application	List	index* (p. 1133)		
ListFaqs	Grants permission to list the Faqs	List	index* (p. 1133)		
ListGroupsOlderThanOrderingId	Grants permission to list groups that are older than an ordering id	List	index* (p. 1133)		
			data-source (p. 1133)		
ListIndices	Grants permission to list the indexes	List			
ListQuerySuggestions	Grants permission to list the QuerySuggestions BlockLists	List	index* (p. 1133)		
ListTagsForResource	Grants permission to list tags for a resource	Read	data-source (p. 1133)		
			faq (p. 1133)		
			index (p. 1133)		
			query-suggestions-block-list (p. 1133)		
			thesaurus (p. 1133)		
ListThesauri	Grants permission to list the Thesauri	List	index* (p. 1133)		
PutPrincipalMapping	Grants permission to put principal mapping in index	Write	index* (p. 1133)		
			data-source (p. 1133)		
Query	Grants permission to query documents and faqs	Read	index* (p. 1133)		
StartDataSourceSyncJob	Grants permission to start Data Source sync job	Write	data-source* (p. 1133)		
			index* (p. 1133)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopDataSourceSync	Grants permission to stop Data Source sync job	Write	data-source* (p. 1133)		
	index* (p. 1133)				
SubmitFeedback	Grants permission to send feedback about a query results	Write	index* (p. 1133)		
TagResource	Grants permission to tag a resource with given key value pairs	Tagging	data-source (p. 1133)		
	faq (p. 1133)				
	index (p. 1133)				
	query-suggestions-block-list (p. 1133)				
	thesaurus (p. 1133)				
	aws:RequestTag/\${TagKey} (p. 1134)				
	aws:TagKeys (p. 1134)				
UntagResource	Grants permission to remove the tag with the given key from a resource	Tagging	data-source (p. 1133)		
	faq (p. 1133)				
	index (p. 1133)				
	query-suggestions-block-list (p. 1133)				
	thesaurus (p. 1133)				
			aws:TagKeys (p. 1134)		
	Grants permission to update a data source		data-source* (p. 1133)		
UpdateExperience	Updates your Amazon Kendra experience such as a search application	Write	index* (p. 1133)		
UpdateIndex	Grants permission to update an Index	Write	index* (p. 1133)		
UpdateQuerySuggestionsBlockList	Grants permission to update a QuerySuggestions BlockList	Write	index* (p. 1133)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			query-suggestions-block-list* (p. 1133)		
UpdateQuerySuggestions	Grants permission to update the query suggestions configuration for an index	Write	index* (p. 1133)		
UpdateThesaurus	Grants permission to update a thesaurus	Write	index* (p. 1133) thesaurus* (p. 1133)		

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 \(p. 1127\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1134)
data-source	arn:\${Partition}:kendra:\${Region}: \${Account}:index/\${IndexId}/data-source/ \${DataSourceId}	aws:ResourceTag/ \${TagKey} (p. 1134)
faq	arn:\${Partition}:kendra:\${Region}: \${Account}:index/\${IndexId}/faq/\${FaqId}	aws:ResourceTag/ \${TagKey} (p. 1134)
experience	arn:\${Partition}:kendra:\${Region}: \${Account}:index/\${IndexId}/experience/ \${ExperienceId}	
thesaurus	arn:\${Partition}:kendra:\${Region}: \${Account}:index/\${IndexId}/thesaurus/ \${ThesaurusId}	aws:ResourceTag/ \${TagKey} (p. 1134)
query-suggestions-block-list	arn:\${Partition}:kendra:\${Region}: \${Account}:index/\${IndexId}/ query-suggestions-block-list/ \${QuerySuggestionsBlockListId}	aws:ResourceTag/ \${TagKey} (p. 1134)

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters access based on the tags that are passed in the request	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters access based on the tags associated with the resource	String
<code>aws:TagKeys</code>	Filters access based on 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 \(p. 1134\)](#)
- [Resource types defined by AWS Key Management Service \(p. 1143\)](#)
- [Condition keys for AWS Key Management Service \(p. 1144\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1144)		
				kms:CallerAccount (p. 1144)	
				kms:ViaService (p. 1146)	
ConnectCustomKeyStore	Controls permission to connect a custom key store to its associated AWS CloudHSM cluster	Write		kms:CallerAccount (p. 1144)	
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* (p. 1143)		
			key* (p. 1144)		
				kms:CallerAccount (p. 1144)	
CreateCustomKeyStore	Controls permission to create a custom key store that is associated with an AWS CloudHSM cluster that you own and manage	Write		kms:CallerAccount (p. 1144)	cloudhsm:DescribeClusters (p. 1144) iam:CreateServiceLinkedRole (p. 1144)
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* (p. 1144)		
				kms:CallerAccount (p. 1144)	
				kms:EncryptionContext: \${EncryptionContextKey} (p. 1145)	
				kms:EncryptionContextKeys (p. 1145)	
				kms:GrantConstraintType (p. 1145)	
				kms:GranteePrincipal (p. 1145)	
				kms:GrantIsForAWSResource (p. 1145)	
				kms:GrantOperations (p. 1145)	
				kms:RetiringPrincipal (p. 1146)	
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} (p. 1144)	iam:CreateServiceLinkedRole (p. 1144)
					kms:PutKeyPolicy
				aws:RequestTag/ \${TagKey} (p. 1144)	kms:TagResource
				aws:TagKeys (p. 1144)	
					kms:BypassPolicyLockoutSafetyCheck
					kms:CallerAccount (p. 1144)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					kms:KeySpec (p. 1145) kms:KeyUsage (p. 1145) kms:KeyOrigin (p. 1145) kms:MultiRegion (p. 1145) kms:MultiRegionKeyType (p. 1146) kms:ViaService (p. 1146)
Decrypt	Controls permission to decrypt ciphertext that was encrypted under an AWS KMS key	Write	key* (p. 1144) kms:CallerAccount (p. 1144) kms:EncryptionAlgorithm (p. 1144) kms:EncryptionContext: \${EncryptionContextKey} (p. 1145) kms:EncryptionContextKeys (p. 1145) kms:RecipientAttestation:ImageSha384 (p. 1145) kms:RequestAlias (p. 1146) kms:ViaService (p. 1146)		
DeleteAlias	Controls permission to delete an alias. Aliases are optional friendly names that you can associate with AWS KMS keys	Write	alias* (p. 1143) key* (p. 1144) kms:CallerAccount (p. 1144) kms:ViaService (p. 1146)		
DeleteCustomKeyStore	Controls permission to delete a custom key store	Write			kms:CallerAccount (p. 1144)
DeleteImportedKeyMaterial	Controls permission to delete cryptographic material that you imported into an AWS KMS key. This action makes the key unusable	Write	key* (p. 1144) kms:CallerAccount (p. 1144) kms:ViaService (p. 1146)		
DescribeCustomKeyStores	Controls permission to view detailed information about custom key stores in the account and region	Read			kms:CallerAccount (p. 1144)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeKey	Controls permission to view detailed information about an AWS KMS key	Read	key* (p. 1144)		
				kms:CallerAccount (p. 1144)	
				kms:RequestAlias (p. 1146)	
DisableKey	Controls permission to disable an AWS KMS key, which prevents it from being used in cryptographic operations	Write	key* (p. 1144)		
				kms:CallerAccount (p. 1144)	
				kms:ViaService (p. 1146)	
DisableKeyRotation	Controls permission to disable automatic rotation of a customer managed AWS KMS key	Write	key* (p. 1144)		
				kms:CallerAccount (p. 1144)	
				kms:ViaService (p. 1146)	
DisconnectCustomKeyStore	Controls permission to disconnect the custom key store from its associated AWS CloudHSM cluster	Write		kms:CallerAccount (p. 1144)	
				kms:ViaService (p. 1146)	
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* (p. 1144)		
				kms:CallerAccount (p. 1144)	
				kms:ViaService (p. 1146)	
EnableKeyRotation	Controls permission to enable automatic rotation of the cryptographic material in an AWS KMS key	Write	key* (p. 1144)		
				kms:CallerAccount (p. 1144)	
				kms:ViaService (p. 1146)	
Encrypt	Controls permission to use the specified AWS KMS key to encrypt data and data keys	Write	key* (p. 1144)		
				kms:CallerAccount (p. 1144)	
				kms:EncryptionAlgorithm (p. 1144)	
				kms:EncryptionContext: \${EncryptionContextKey} (p. 1145)	
				kms:EncryptionContextKeys (p. 1145)	
				kms:RequestAlias (p. 1146)	
				kms:ViaService (p. 1146)	

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* (p. 1144)		
GenerateDataKey	Controls permission to use the AWS KMS key to generate data key pairs	Write	key* (p. 1144)		
GenerateDataKey	Controls permission to use the AWS KMS key to generate data key pairs. Unlike the <code>GenerateDataKeyValuePair</code> operation, this operation returns an encrypted private key without a plaintext copy	Write	key* (p. 1144)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GenerateDataKey	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* (p. 1144)		
				kms:CallerAccount (p. 1144)	
				kms:EncryptionAlgorithm (p. 1144)	
				kms:EncryptionContext: \${EncryptionContextKey} (p. 1145)	
				kms:EncryptionContextKeys (p. 1145)	
				kms:RequestAlias (p. 1146)	
				kms:ViaService (p. 1146)	
			key* (p. 1144)		
				kms:CallerAccount (p. 1144)	
				kms:MacAlgorithm (p. 1145)	
				kms:RequestAlias (p. 1146)	
				kms:ViaService (p. 1146)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions	
ImportKeyMaterial	Controls permission to import cryptographic material into an AWS KMS key	Write	key* (p. 1144)			
				kms:CallerAccount (p. 1144)		
				kms:ExpirationModel (p. 1145)		
				kms:ValidTo (p. 1146)		
				kms:ViaService (p. 1146)		
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				
			key* (p. 1144)			
				kms:CallerAccount (p. 1144)		
				kms:GrantIsForAWSResource (p. 1145)		
				kms:ViaService (p. 1146)		
ListKeyPolicies	Controls permission to view the names of key policies for an AWS KMS key	List	key* (p. 1144)			
				kms:CallerAccount (p. 1144)		
				kms:ViaService (p. 1146)		
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* (p. 1144)			
					kms:CallerAccount (p. 1144)	
				kms:ViaService (p. 1146)		
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	key* (p. 1144)			
PutKeyPolicy	Controls permission to replace the key policy for the specified AWS KMS key	Permissions management	key* (p. 1144)			
					kms:BypassPolicyLockoutSafetyCheck	
					kms:CallerAccount (p. 1144)	
				kms:ViaService (p. 1146)		

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* (p. 1144)	kms:CallerAccount (p. 1144) kms:EncryptionAlgorithm (p. 1144) kms:EncryptionContext: \${EncryptionContextKey} (p. 1145) kms:EncryptionContextKeys (p. 1145) kms:ReEncryptOnSameKey (p. 1146) kms:RequestAlias (p. 1146) kms:ViaService (p. 1146)	
ReEncryptTo	Controls permission to encrypt data as part of the process that decrypts and reencrypts the data within AWS KMS	Write	key* (p. 1144)	kms:CallerAccount (p. 1144) kms:EncryptionAlgorithm (p. 1144) kms:EncryptionContext: \${EncryptionContextKey} (p. 1145) kms:EncryptionContextKeys (p. 1145) kms:ReEncryptOnSameKey (p. 1146) kms:RequestAlias (p. 1146) kms:ViaService (p. 1146)	
ReplicateKey	Controls permission to replicate a multi-Region primary key	Write	key* (p. 1144)	iam:CreateServiceLinkedRole kms>CreateKey kms:PutKeyPolicy kms:TagResource	kms:CallerAccount (p. 1144) kms:ReplicaRegion (p. 1146) kms:ViaService (p. 1146)
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* (p. 1144)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RevokeGrant	Controls permission to revoke a grant, which denies permission for all operations that depend on the grant	Permissions management	key* (p. 1144)	kms:CallerAccount (p. 1144)	kms:GrantIsForAWSResource (p. 1145) kms:ViaService (p. 1146)
ScheduleKeyDelete	Controls permission to schedule deletion of an AWS KMS key	Write	key* (p. 1144)	kms:CallerAccount (p. 1144)	kms:ViaService (p. 1146)
Sign	Controls permission to produce a digital signature for a message	Write	key* (p. 1144)	kms:CallerAccount (p. 1144)	kms:MessageType (p. 1145) kms:RequestAlias (p. 1146) kms:SigningAlgorithm (p. 1146) kms:ViaService (p. 1146)
SynchronizeMultiRegionKeys [permission only]	Controls access to internal APIs that synchronize multi-Region keys	Write	key* (p. 1144)		
TagResource	Controls permission to create or update tags that are attached to an AWS KMS key	Tagging	key* (p. 1144)	aws:RequestTag/ \${TagKey} (p. 1144)	aws:TagKeys (p. 1144) kms:CallerAccount (p. 1144) kms:ViaService (p. 1146)
UntagResource	Controls permission to delete tags that are attached to an AWS KMS key	Tagging	key* (p. 1144)	aws:TagKeys (p. 1144)	kms:CallerAccount (p. 1144) kms:ViaService (p. 1146)
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* (p. 1143) key* (p. 1144)	kms:CallerAccount (p. 1144)	kms:ViaService (p. 1146)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateCustomKeyProperties	Controls permission to change the properties of a custom key store	Write		kms:CallerAccount (p. 1144)	
UpdateKeyDescription	Controls permission to delete or change the description of an AWS KMS key	Write	key* (p. 1144)	kms:CallerAccount (p. 1144) kms:ViaService (p. 1146)	
UpdatePrimaryRegion	Controls permission to update the primary Region of a multi-Region primary key	Write	key* (p. 1144)	kms:CallerAccount (p. 1144) kms:PrimaryRegion (p. 1146) kms:ViaService (p. 1146)	
Verify	Controls permission to use the specified AWS KMS key to verify digital signatures	Write	key* (p. 1144)	kms:CallerAccount (p. 1144) kms:MessageType (p. 1145) kms:RequestAlias (p. 1146) kms:SigningAlgorithm (p. 1146) kms:ViaService (p. 1146)	
VerifyMac	Controls permission to use the AWS KMS key to verify message authentication codes	Write	key* (p. 1144)	kms:CallerAccount (p. 1144) kms:MacAlgorithm (p. 1145) kms:RequestAlias (p. 1146) kms:ViaService (p. 1146)	

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 \(p. 1134\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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}	

Resource types	ARN	Condition keys
key	<code>arn:\${Partition}:kms:\${Region}:\${Account}:key/\${KeyId}</code>	aws:ResourceTag/\${TagKey} (p. 1144) kms:KeyOrigin (p. 1145) kms:KeySpec (p. 1145) kms:KeyUsage (p. 1145) kms:MultiRegion (p. 1145) kms:MultiRegionKeyType (p. 1146) kms:ResourceAliases (p. 1146)

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 [Available global condition 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:DataKeySpec	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	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 pair	String
kms:EncryptionContextKey	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 pair	ArrayOfString
kms:ExpirationModel	Filters access to the ImportKeyMaterial operation based on the value of the ExpirationModel parameter in the request	String
kms:GrantConstraint	Filters access to the CreateGrant operation based on the 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: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
kms:KeySpec	Filters access to an API operation based on theKeySpec 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 theKeyUsage 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

Condition keys	Description	Type
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
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:RecipientAttestationHash	Filters access to the Decrypt, GenerateDataKey, and GenerateRandom operations based on the image hash in the attestation document in the request	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: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 \(for Apache Cassandra\) \(p. 1147\)](#)
- [Resource types defined by Amazon Keyspaces \(for Apache Cassandra\) \(p. 1148\)](#)
- [Condition keys for Amazon Keyspaces \(for Apache Cassandra\) \(p. 1149\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 (p. 1148)		
			table (p. 1148)		
				aws:RequestTag/\${TagKey} (p. 1149)	
				aws:TagKeys (p. 1149)	
Create	Grants permission to create a keyspace or table	Write	keyspace (p. 1148)		
			table (p. 1148)		
				aws:RequestTag/\${TagKey} (p. 1149)	
				aws:TagKeys (p. 1149)	
Drop	Grants permission to drop a keyspace or table	Write	keyspace (p. 1148)		
			table (p. 1148)		
Modify	Grants permission to INSERT, UPDATE or DELETE data in a table	Write	table* (p. 1148)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Restore	Grants permission to restore table from a backup	Write	table* (p. 1148)		
				aws:RequestTag/ \${TagKey} (p. 1149)	aws:TagKeys (p. 1149)
Select	Grants permission to SELECT data from a table	Read	table* (p. 1148)		
TagResource	Grants permission to tag a keyspace or table	Tagging	keyspace (p. 1148)		
			table (p. 1148)		
				aws:RequestTag/ \${TagKey} (p. 1149)	
UntagResource	Grants permission to untag a keyspace or table	Tagging	keyspace (p. 1148)		
			table (p. 1148)		
				aws:RequestTag/ \${TagKey} (p. 1149)	
UpdatePartitioner	Grants permission to UPDATE the partitioner in a system table	Write	table* (p. 1148)		

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 \(p. 1147\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1149)
table	arn:\${Partition}:cassandra:\${Region}: \${Account}:/keyspace/\${KeyspaceName}/table/ \${TableName}	aws:ResourceTag/ \${TagKey} (p. 1149)

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 [Available global condition keys](#).

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

Actions, resources, and condition keys for Amazon Kinesis

Amazon Kinesis (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 \(p. 1149\)](#)
- [Resource types defined by Amazon Kinesis \(p. 1152\)](#)
- [Condition keys for Amazon Kinesis \(p. 1153\)](#)

Actions defined by Amazon Kinesis

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

The **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 10 tags	Tagging	stream* (p. 1152)		
CreateStream	Grants permission to create a Amazon Kinesis stream	Write	stream* (p. 1152)		
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* (p. 1152)		
DeleteStream	Grants permission to delete a stream and all its shards and data	Write	stream* (p. 1152)		
DeregisterStreamConsumer	Grants permission to deregister a stream consumer with a Kinesis data stream	Write	consumer* (p. 1152)		
DescribeLimits	Grants permission to describe the shard limits and usage for the account	Read			
DescribeStream	Grants permission to describe the specified stream	Read	stream* (p. 1152)		
DescribeStreamConsumer	Grants permission to get the description of a registered stream consumer	Read	consumer* (p. 1152)		
DescribeStreamSummary	Grants permission to provide a summarized description of the specified Kinesis data stream without the shard list	Read	stream* (p. 1152)		
DisableEnhancedMonitoring	Grants permission to disable 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* (p. 1152)		
GetShardIterator	Grants permission to get a shard iterator. A shard iterator expires five minutes after it is returned to the requester	Read	stream* (p. 1152)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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* (p. 1152)		
ListShards	Grants permission to list the shards in a stream and provides information about each shard	List			
ListStreamConsumers	Grants permission to list the consumers registered to receive data from a Kinesis stream using enhanced fan-out, and provides information about each consumer	List	stream* (p. 1152)		
ListStreams	Grants permission to list your streams	List			
ListTagsForStream	Grants permission to list the tags for the specified Amazon Kinesis stream	Read	stream* (p. 1152)		
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* (p. 1152)		
PutRecord	Grants permission to write a single data record from a producer into an Amazon Kinesis stream	Write	stream* (p. 1152)		
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* (p. 1152)		
RegisterStreamConsumer	Grants permission to register a consumer with a Kinesis data stream	Write	stream* (p. 1152)		
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* (p. 1152)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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* (p. 1152)		
StartStreamEncryption UpdateStreamEncryption	Grants permission to enable or update server-side encryption using an AWS KMS key for a specified stream	Write	kmsKey* (p. 1152)		
			stream* (p. 1152)		
StopStreamEncryption UpdateStreamEncryption	Grants permission to disable server-side encryption for a specified stream	Write	kmsKey* (p. 1152)		
			stream* (p. 1152)		
SubscribeToShard	Grants permission to listen to a specific shard with enhanced fan-out	Read	consumer* (p. 1152)		
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			

Resource types defined by Amazon Kinesis

The following resource types are defined by this service and can be used in the Resource element of IAM permission policy statements. Each action in the [Actions table \(p. 1149\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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}	
consumer	arn:\${Partition}:kinesis: \${Region}: \${Account}: \${StreamType}/ \${StreamName}/consumer/\${ConsumerName}: \${ConsumerCreationTimestamp}	
kmsKey	arn:\${Partition}:kms:\${Region}: \${Account}:key/\${KeyId}	

Condition keys for Amazon Kinesis

Kinesis 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 [Available keys for conditions](#).

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 \(p. 1153\)](#)
- [Resource types defined by Amazon Kinesis Analytics \(p. 1155\)](#)
- [Condition keys for Amazon Kinesis Analytics \(p. 1155\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddApplicationInput	Adds input to the application.	Write	application* (p. 1155)		
AddApplicationOutput	Adds output to the application.	Write	application* (p. 1155)		
AddApplicationReference	Adds reference data source to the application	Write	application* (p. 1155)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateApplication	Creates an application.	Write		aws:RequestTag/ \${TagKey} (p. 1155) aws:TagKeys (p. 1155)	
DeleteApplication	Deletes the application.	Write	application* (p. 1155)		
DeleteApplicationOutput	Deletes the specified output of the application.	Write	application* (p. 1155)		
DeleteApplicationDataSource	Deletes the specified reference data source of the application.	Write	application* (p. 1155)		
DescribeApplication	Describes the specified application.	Read	application* (p. 1155)		
DiscoverInputSchema	Discovers the input schema for the application.	Read			
GetApplicationStream [permission only]	Grant permission to Kinesis Data Analytics console to display stream results for Kinesis Data Analytics SQL runtime applications.	Read	application* (p. 1155)		
ListApplications	List applications for the account	List			
ListTagsForResource	Fetch the tags associated with the application.	Read	application* (p. 1155)		
StartApplication	Starts the application.	Write	application* (p. 1155)		
StopApplication	Stops the application.	Write	application* (p. 1155)		
TagResource	Add tags to the application.	Tagging	application* (p. 1155)		
			aws:RequestTag/ \${TagKey} (p. 1155) aws:TagKeys (p. 1155)		
UntagResource	Remove the specified tags from the application.	Tagging	application* (p. 1155)		
			aws:TagKeys (p. 1155)		
UpdateApplication	Updates the application.	Write	application* (p. 1155)		

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 \(p. 1153\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
application	<code>arn:\${Partition}:kinesisanalytics:\${Region}: \${Account}:application/\${ApplicationName}</code>	<code>aws:ResourceTag/ \${TagKey} (p. 1155)</code>

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/ \${TagKey}</code>	Filters actions based on the allowed set of values for each of the tags	String
<code>aws:ResourceTag/ \${TagKey}</code>	Filters actions based on tag-value associated with the resource	String
<code>aws:TagKeys</code>	Filters actions based on the presence of mandatory tag keys in the request	String

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 \(p. 1156\)](#)
- [Resource types defined by Amazon Kinesis Analytics V2 \(p. 1158\)](#)
- [Condition keys for Amazon Kinesis Analytics V2 \(p. 1158\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 <code>CloudWatchLoggingOption</code> to the application	Write	application* (p. 1158)		
AddApplicationInput	Grants permission to add input <code>to</code> the application	Write	application* (p. 1158)		
AddApplicationInputProcessingConfiguration	Grants permission to add input <code>processingConfiguration</code> to the application	Write	application* (p. 1158)		
AddApplicationOutput	Grants permission to add output <code>to</code> the application	Write	application* (p. 1158)		
AddApplicationReferenceDataSource	Grants permission to add <code>referenceDataSource</code> to the application	Write	application* (p. 1158)		
AddApplicationVpcConfiguration	Grants permission to add VPC <code>vpcConfiguration</code> to the application	Write	application* (p. 1158)		
CreateApplication	Grants permission to create an application	Write		<code>aws:RequestTag/\${TagKey}</code> (p. 1158) <code>aws:TagKeys</code> (p. 1159)	
CreateApplicationReturnAddress	Grants permission to create and <code>returnAddress</code> that you can use to connect to an application's extension	Read	application* (p. 1158)		
CreateApplicationSnapshot	Grants permission to create a <code>snapshot</code> for an application	Write	application* (p. 1158)		
DeleteApplication	Grants permission to delete the application	Write	application* (p. 1158)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteApplicationCloudWatchLogging	Grants permission to delete the specified CloudWatch Logging option of the application	Write	application* (p. 1158)		
DeleteApplicationIngestionConfiguration	Grants permission to delete the specified Ingestion Configuration configuration of the application	Write	application* (p. 1158)		
DeleteApplicationOutput	Grants permission to delete the specified output of the application	Write	application* (p. 1158)		
DeleteApplicationReferenceDataSource	Grants permission to delete the specified Reference Data Source of the application	Write	application* (p. 1158)		
DeleteApplicationSnapshot	Grants permission to delete a snapshot for an application	Write	application* (p. 1158)		
DeleteApplicationVPCConfiguration	Grants permission to delete the specified VPC Configuration of the application	Write	application* (p. 1158)		
DescribeApplication	Grants permission to describe the specified application	Read	application* (p. 1158)		
DescribeApplicationSnapshot	Grants permission to describe an application snapshot	Read	application* (p. 1158)		
DescribeApplicationVersion	Grants permission to describe the application version of an application	Read	application* (p. 1158)		
DiscoverInputSchema	Grants permission to discover the input schema for the application	Read			
ListApplicationSnapshots	Grants permission to list the snapshots for an application	Read	application* (p. 1158)		
ListApplicationVersions	Grants permission to list application versions of an application	Read	application* (p. 1158)		
ListApplications	Grants permission to list applications for the account	List			
ListTagsForResource	Grants permission to fetch the tags associated with the application	Read	application* (p. 1158)		
RollbackApplication	Grants permission to perform a rollback operation on an application	Write	application* (p. 1158)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartApplication	Grants permission to start the application	Write	application* (p. 1158)		
StopApplication	Grants permission to stop the application	Write	application* (p. 1158)		
TagResource	Grants permission to add tags to the application	Tagging	application* (p. 1158)		
				aws:RequestTag/\${TagKey} (p. 1158)	
				aws:TagKeys (p. 1159)	
UntagResource	Grants permission to remove the specified tags from the application	Tagging	application* (p. 1158)		
				aws:TagKeys (p. 1159)	
UpdateApplication	Grants permission to update the application	Write	application* (p. 1158)		
UpdateApplicationMaintenanceConfiguration	Grants permission to update the maintenance configuration of an application	Write	application* (p. 1158)		

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 \(p. 1156\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
application	<code>arn:\${Partition}:kinesisanalytics:\${Region}:\${Account}:application/\${ApplicationName}</code>	aws:ResourceTag/\${TagKey} (p. 1159)

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 [Available global condition keys](#).

Condition keys	Description	Type
aws:RequestTag/\${TagKey}	Filters actions based on the allowed set of values for each of the tags	String

Condition keys	Description	Type
<code>aws:ResourceTag/\${TagKey}</code>	Filters actions based on tag-value associated with the resource	String
<code>aws:TagKeys</code>	Filters actions based on the presence of mandatory tag keys in the request	String

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 \(p. 1159\)](#)
- [Resource types defined by Amazon Kinesis Firehose \(p. 1160\)](#)
- [Condition keys for Amazon Kinesis Firehose \(p. 1161\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
<code>CreateDeliveryStream</code>	Grants permission to create a delivery stream	Write	<code>deliverystream*</code> (p. 1161)	<code>aws:RequestTag/\${TagKey}</code> (p. 1161)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					aws:TagKeys (p. 1161)
DeleteDeliveryStream	Grants permission to delete a delivery stream and its data	Write	deliverystream* (p. 1161)		
DescribeDeliveryStream	Grants permission to describe the specified delivery stream and gets the status	Read	deliverystream* (p. 1161)		
ListDeliveryStreams	Grants permission to list your delivery streams	List			
ListTagsForDeliveryStream	Grants permission to list the tags for the specified delivery stream	List	deliverystream* (p. 1161)		
PutRecord	Grants permission to write a single data record into an Amazon Kinesis Firehose delivery stream	Write	deliverystream* (p. 1161)		
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* (p. 1161)		
StartDeliveryStream	Grants permission to enable server-side encryption (SSE) for the delivery stream	Write	deliverystream* (p. 1161)		
StopDeliveryStream	Grants permission to disable the specified destination of the specified delivery stream	Write	deliverystream* (p. 1161)		
TagDeliveryStream	Grants permission to add or update tags for the specified delivery stream	Tagging	deliverystream* (p. 1161)		
				aws:RequestTag/ \${TagKey} (p. 1161)	aws:TagKeys (p. 1161)
UntagDeliveryStream	Grants permission to remove tags from the specified delivery stream	Tagging	deliverystream* (p. 1161)		
					aws:TagKeys (p. 1161)
UpdateDestination	Grants permission to update the specified destination of the specified delivery stream	Write	deliverystream* (p. 1161)		

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 \(p. 1159\)](#) identifies the resource

types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1161)

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 [Available global condition 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 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 \(p. 1161\)](#)
- [Resource types defined by Amazon Kinesis Video Streams \(p. 1164\)](#)
- [Condition keys for Amazon Kinesis Video Streams \(p. 1165\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1164)		
ConnectAsViewer	Grants permission to connect as a viewer to the signaling channel specified by the endpoint	Write	channel* (p. 1164)		
CreateSignalingChannel	Grants permission to create a signaling channel	Write	channel* (p. 1164)	aws:RequestTag/ \${TagKey} (p. 1165) aws:TagKeys (p. 1165)	
CreateStream	Grants permission to create a Kinesis video stream	Write	stream* (p. 1164)		
				aws:RequestTag/ \${TagKey} (p. 1165)	
				aws:TagKeys (p. 1165)	
DeleteSignalingChannel	Grants permission to delete an existing signaling channel	Write	channel* (p. 1164)		
DeleteStream	Grants permission to delete an existing Kinesis video stream	Write	stream* (p. 1164)		
DescribeSignalingChannel	Grants permission to describe the specified signaling channel	List	channel* (p. 1164)		
DescribeStream	Grants permission to describe the specified Kinesis video stream	List	stream* (p. 1164)		
GetClip	Grants permission to get a media clip from a video stream	Read	stream* (p. 1164)		
GetDASHStreamingURLs	Grants permission to create URLs for MP4-DASH video streaming	Read	stream* (p. 1164)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDataEndpoint	Grants permission to get an endpoint for a specified stream for either reading or writing media data to Kinesis Video Streams	Read	stream* (p. 1164)		
GetHLSStreamingURLsForHLS	Grants permission to create a URL for HLS video streaming	Read	stream* (p. 1164)		
GetIceServerConfig	Grants permission to get the ICE server configuration	Read	channel* (p. 1164)		
GetMedia	Grants permission to return media content of a Kinesis video stream	Read	stream* (p. 1164)		
GetMediaForFragment	Grants permission to read and return media data only from persisted storage	Read	stream* (p. 1164)		
GetSignalingChannelEndpoints	Grants permission to get endpoints for a specified combination of protocol and role for a signaling channel	Read	channel* (p. 1164)		
ListFragments	Grants permission to list the fragments from archival storage based on the pagination token or selector type with range specified	List	stream* (p. 1164)		
ListSignalingChannels	Grants permission to list your signaling channels	List			
ListStreams	Grants permission to list your Kinesis video streams	List			
ListTagsForResource	Grants permission to fetch the tags associated with your resource	Read	channel (p. 1164)		
ListTagsForStream	Grants permission to fetch the tags associated with Kinesis video stream		stream (p. 1164)		
PutMedia	Grants permission to send media data to a Kinesis video stream	Write	stream* (p. 1164)		
SendAlexaOfferToAlexa	Grants permission to send the SDP offer to the master	Write	channel* (p. 1164)		
TagResource	Grants permission to attach set of tags to your resource	Tagging	channel (p. 1164)		
			stream (p. 1164)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 1165) aws:TagKeys (p. 1165)	
TagStream	Grants permission to attach set of tags to your Kinesis video streams	Tagging	stream* (p. 1164)		
				aws:RequestTag/ \${TagKey} (p. 1165) aws:TagKeys (p. 1165)	
UntagResource	Grants permission to remove one or more tags from your resource	Tagging	channel (p. 1164)		
			stream (p. 1164)		
				aws:TagKeys (p. 1165)	
UntagStream	Grants permission to remove one or more tags from your Kinesis video streams	Tagging	stream* (p. 1164)		
				aws:TagKeys (p. 1165)	
UpdateDataRetention	Grants permission to update the data retention period of your Kinesis video stream	Write	stream* (p. 1164)		
UpdateSignalingChannel	Grants permission to update an existing signaling channel	Write	channel* (p. 1164)		
UpdateStream	Grants permission to update an existing Kinesis video stream	Write	stream* (p. 1164)		

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 \(p. 1161\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1165)
channel	arn:\${Partition}:kinesisvideo:\${Region}: \${Account}:channel/\${ChannelName}/ \${CreationTime}	aws:ResourceTag/ \${TagKey} (p. 1165)

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters requests based on the allowed set of values for each of the tags	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters actions based on tag-value associated with the stream	String
<code>aws:TagKeys</code>	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 \(p. 1165\)](#)
- [Resource types defined by AWS Lake Formation \(p. 1168\)](#)
- [Condition keys for AWS Lake Formation \(p. 1168\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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			
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			
DeleteDataCellsFilter	Grants permission to delete a Lake Formation data cell filter	Write			
DeleteLFTag	Grants permission to delete a Lake Formation tag	Write			
DeleteObjectsOnTable	Grants permission to delete the specified objects if the transaction is canceled	Write			
DeregisterResource	Grants permission to deregister a registered location	Write			
DescribeResource	Grants permission to describe a registered location	Read			
DescribeTransaction	Grants permission to get status of the given transaction	Read			
ExtendTransaction	Grants permission to extend the timeout of the given transaction	Write			
GetDataAccess	Grants permission to virtual data lake access	Write			
GetDataLakeSettings	Grants permission to retrieve data lake settings such as the list of data lake administrators and database and table default permissions	Read			

Service Authorization Reference
Service Authorization Reference
AWS Lake Formation

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetEffectivePermissionsPath	Grants permission to retrieve permissions attached to resources in the given path	Read			
GetLFTag	Grants permission to retrieve a Lake Formation tag	Read			
GetQueryState	Grants permission to retrieve the state of the given query	Read			lakeformation:StartQuery
GetQueryStatistics	Grants permission to retrieve the statistics for the given query	Read			lakeformation:StartQuery
GetResourceLFTags	Grants permission to retrieve LakeFormation tags on a catalog resource	Read			
GetTableObjects	Grants permission to retrieve objects from a table	Read			
GetWorkUnitResults	Grants permission to retrieve the results for the given work units	Read			lakeformation:GetWorkUnits
GetWorkUnits	Grants permission to retrieve the work units for the given query	Read			lakeformation:StartQuery
GrantPermissions	Grants permission to data lake permissions to a principal	Permissions management			
ListDataCellsFilters	Grants permission to list cell filters	List			
ListLFTags	Grants permission to list Lake Formation tags	Read			
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 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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterResource	Grants permission to register a new location to be managed by Lake Formation	Write			
RemoveLFTagsFromLakeFormation	Grants permission to remove Lake Formation tags from catalog resources	Tagging			
RevokePermissions	Grants permission to revoke data lake permissions from a principal	Permissions management			
SearchDatabasesByTags	Grants permission to list catalog databases with Lake Formation tags	Read			
SearchTablesByTags	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			
UpdateLFTag	Grants permission to update a Lake Formation tag	Write			
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			
UpdateTableStorageConfiguration	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

Lake Formation 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 [Available keys for conditions](#).

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 \(p. 1169\)](#)
- [Resource types defined by AWS Lambda \(p. 1175\)](#)
- [Condition keys for AWS Lambda \(p. 1176\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 <code>permissions</code> to the resource-based policy of a version of an AWS Lambda layer	Permissions management	layerVersion* (p. 1176)		
AddPermission	Grants permission to give an AWS service or another account permission to use an AWS Lambda function	Permissions management	function* (p. 1175)	lambda:Principal (p. 1176) lambda:FunctionUrlAuthType (p. 1176)	
CreateAlias	Grants permission to create an alias for a Lambda function version	Write	function* (p. 1175)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCodeSigningConfig	Grants permission to create an AWS Lambda code signing config	Write			
CreateEventSourceMapping	Grants permission to create a mapping between an event source and an AWS Lambda function	Write		lambda:FunctionArn (p. 1176)	
CreateFunction	Grants permission to create an AWS Lambda function	Write	function* (p. 1175)		
			lambda:Layer (p. 1176)		
			lambda:VpcIds (p. 1176)		
			lambda:SubnetIds (p. 1176)		
			lambda:SecurityGroupIds (p. 1176)		
CreateFunctionUrlConfig	Grants permission to create a url configuration for a Lambda function	Write	function* (p. 1175)		
				lambda:FunctionUrlAuthType (p. 1176)	
				lambda:FunctionArn (p. 1176)	
DeleteAlias	Grants permission to delete an AWS Lambda function alias	Write	function* (p. 1175)		
DeleteCodeSigningConfig	Grants permission to delete an AWS Lambda code signing config	Write	code signing config* (p. 1175)		
				eventSourceMapping* (p. 1175)	
DeleteEventSourceMapping	Grants permission to delete an AWS Lambda event source mapping	Write		lambda:FunctionArn (p. 1176)	
DeleteFunction	Grants permission to delete an AWS Lambda function	Write	function* (p. 1175)		
DeleteFunctionCodeSigningConfig	Grants permission to detach a code signing config from an AWS Lambda function	Write	function* (p. 1175)		
DeleteFunctionConcurrencyConfig	Grants permission to remove a concurrent execution limit from an AWS Lambda function	Write	function* (p. 1175)		
DeleteFunctionEventConfiguration	Grants permission to delete the configuration for asynchronous invocation for an AWS Lambda function, version, or alias	Write	function* (p. 1175)		
DeleteFunctionUrlConfig		Write	function* (p. 1175)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to delete function url configuration for a Lambda function			lambda:FunctionUrlAuthType (p. 1176)	
DeleteLayerVersion	Grants permission to delete a version of an AWS Lambda layer	Write	layerVersion* (p. 1176)		
DeleteProvisionedConcurrency	Grants permission to delete the provisioned concurrency configuration for an AWS Lambda function	Write	function alias (p. 1175)		
			function version (p. 1175)		
DisableReplication [permission only]	Grants permission to disable replication for a Lambda@Edge function	Permissions management	function* (p. 1175)		
EnableReplication [permission only]	Grants permission to enable replication for a Lambda@Edge function	Permissions management	function* (p. 1175)		
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* (p. 1175)		
GetCodeSigningConfig	Grants permission to view details about an AWS Lambda code signing config	Read	code signing config* (p. 1175)		
GetEventSourceMapping	Grants permission to view details about an AWS Lambda event source mapping	Read	eventSourceMapping* (p. 1175)		
				lambda:FunctionArn (p. 1176)	
GetFunction	Grants permission to view details about an AWS Lambda function	Read	function* (p. 1175)		
GetFunctionCodeSigningConfig	Grants permission to view the code signing config arn attached to an AWS Lambda function	Read	function* (p. 1175)		
GetFunctionConcurrency	Grants permission to view details about the reserved concurrency configuration for a function	Read	function* (p. 1175)		
GetFunctionConfigurations	Grants permission to view details about the version-specific settings of an AWS Lambda function or version	Read	function* (p. 1175)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetFunctionEventConfiguration	Grants permission to view the configuration for asynchronous invocation for a function, version, or alias	Read	function* (p. 1175)		
GetFunctionUrlConfig	Grants permission to read function url configuration for a Lambda function	Read	function* (p. 1175)	lambda:FunctionUrlAuthType (p. 1176)	lambda:FunctionArn (p. 1176)
GetLayerVersion	Grants permission to view details about a version of an AWS Lambda layer. Note this action also supports GetLayerVersionByArn API	Read	layerVersion* (p. 1176)		
GetLayerVersionPolicy	Grants permission to view the resource-based policy for a version of an AWS Lambda layer	Read	layerVersion* (p. 1176)		
GetPolicy	Grants permission to view the resource-based policy for an AWS Lambda function, version, or alias	Read	function* (p. 1175)		
GetProvisionedConcurrencyConfig	Grants permission to view the provisioned concurrency configuration for an AWS Lambda function's alias or version	Read	functionalias (p. 1175)	functionversion (p. 1175)	
InvokeAsync	Grants permission to invoke a function asynchronously (Deprecated)	Write	function* (p. 1175)		
InvokeFunction	Grants permission to invoke an AWS Lambda function	Write	function* (p. 1175)		
InvokeFunctionUrl [permission only]	Grants permission to invoke an AWS Lambda function through url	Write	function* (p. 1175)	lambda:FunctionUrlAuthType (p. 1176)	lambda:FunctionArn (p. 1176)
ListAliases	Grants permission to retrieve a list of aliases for an AWS Lambda function	List	function* (p. 1175)		
ListCodeSigningConfigs	Grants permission to retrieve a list of AWS Lambda code signing configs	List			
ListEventSourceMappings	Grants permission to retrieve a list of AWS Lambda event source mappings	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListFunctionEventConfigurations	Grants permission to retrieve a list of configurations for asynchronous invocation for a function	List	function* (p. 1175)		
ListFunctionUrlConfigurations	Grants permission to read function url configurations for a function	List	function* (p. 1175)		
				lambda:FunctionUrlAuthType (p. 1176)	
ListFunctions	Grants permission to retrieve a list of AWS Lambda functions, with the version-specific configuration of each function	List			
ListFunctionsByCodeSigningConfig	Grants permission to retrieve a list of AWS Lambda functions by the code signing config assigned	List	code signing config* (p. 1175)		
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			
ListProvisionedConcurrencyConfigurations	Grants permission to retrieve a list of provisioned concurrency configurations for an AWS Lambda function	List	function* (p. 1175)		
ListTags	Grants permission to retrieve a list of tags for an AWS Lambda function	Read	function* (p. 1175)		
ListVersionsByFunction	Grants permission to retrieve a list of versions for an AWS Lambda function	List	function* (p. 1175)		
PublishLayerVersion	Grants permission to create an AWS Lambda layer	Write	layer* (p. 1175)		
PublishVersion	Grants permission to create an AWS Lambda function version	Write	function* (p. 1175)		
PutFunctionCodeSigningConfig	Grants permission to attach a code signing config to an AWS Lambda function	Write	code signing config* (p. 1175)		
			function* (p. 1175)		
				lambda:CodeSigningConfigArn (p. 1175)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutFunctionConcurrency	Grants permission to configure concurrency for an AWS Lambda function	Write	function* (p. 1175)		
PutFunctionEventInvokeOptions	Grants permission to configures options for asynchronous invocation on an AWS Lambda function, version, or alias	Write	function* (p. 1175)		
PutProvisionedConcurrencyConfig	Grants permission to configure concurrency for an AWS Lambda function's alias or version	Write	function alias (p. 1175)		
			function version (p. 1175)		
RemoveLayerVersionStatement	Grants permission to remove a statement from the permissions policy for a version of an AWS Lambda layer	Permissions management	layerVersion* (p. 1176)		
RemovePermission	Grants permission to revoke function-use permission from an AWS service or another account	Permissions management	function* (p. 1175)	lambda:Principal (p. 1176)	lambda:FunctionUrlAuthType (p. 1176)
TagResource	Grants permission to add tags to an AWS Lambda function	Tagging	function* (p. 1175)		
UntagResource	Grants permission to remove tags from an AWS Lambda function	Tagging	function* (p. 1175)		
UpdateAlias	Grants permission to update the configuration of an AWS Lambda function's alias	Write	function* (p. 1175)		
UpdateCodeSigningConfig	Grants permission to update Lambda code signing config	Write	code signing config* (p. 1175)		
UpdateEventSourceMapping	Grants permission to update the configuration of an AWS Lambda event source mapping	Write	eventSourceMapping* (p. 1175)		
	lambda:FunctionArn (p. 1176)				
UpdateFunctionCode	Grants permission to update the code of an AWS Lambda function	Write	function* (p. 1175)		
UpdateFunctionCodeSigningConfig	Grants permission to update the code signing config of an AWS Lambda function	Write	code signing config* (p. 1175)		
			function* (p. 1175)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateFunctionConfiguration	Grants permission to modify the specific settings of an AWS Lambda function	Write	function* (p. 1175)		
UpdateFunctionEventSourceMapping	Grants permission to modify the configuration for asynchronous invocation for an AWS Lambda function, version, or alias	Write	function* (p. 1175)		
UpdateFunctionUrl	Grants permission to update a function url configuration for a Lambda function	Write	function* (p. 1175)	lambda:FunctionUrlAuthType (p. 1176)	lambda:FunctionArn (p. 1176)

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 \(p. 1169\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
code signing config	<code>arn:\${Partition}:lambda:\${Region}: \${Account}:code-signing-config: \${CodeSigningConfigId}</code>	
eventSourceMapping	<code>arn:\${Partition}:lambda:\${Region}: \${Account}:event-source-mapping:\${UUID}</code>	
function	<code>arn:\${Partition}:lambda:\${Region}: \${Account}:function:\${FunctionName}</code>	
function alias	<code>arn:\${Partition}:lambda:\${Region}: \${Account}:function:\${FunctionName}:\${Alias}</code>	
function version	<code>arn:\${Partition}:lambda:\${Region}: \${Account}:function:\${FunctionName}: \${Version}</code>	
layer	<code>arn:\${Partition}:lambda:\${Region}: \${Account}:layer:\${LayerName}</code>	

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 [Available global condition keys](#).

Condition keys	Description	Type
lambda:CodeSigningConfigArn	Filters access by the ARN of an AWS Lambda code signing configuration.	String
lambda:FunctionArn	Filters access by the ARN of an AWS Lambda function.	ARN
lambda:FunctionUrlArn	Filters access by authorization type specified in the URL. Available during CreateFunctionUrlConfig, UpdateFunctionUrlConfig, DeleteFunctionUrlConfig, GetFunctionUrlConfig, ListFunctionUrlConfig, AddPermission and RemovePermission operations.	String
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: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 Launch Wizard

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](#).

Topics

- [Actions defined by Launch Wizard \(p. 1177\)](#)
- [Resource types defined by Launch Wizard \(p. 1178\)](#)
- [Condition keys for Launch Wizard \(p. 1178\)](#)

Actions defined by 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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteApp [permission only]	Delete an application	Write			
DescribeProvisioningApplications [permission only]	Describe provisioning applications	Read			
DescribeProvisioningEvents [permission only]	Describe provisioning events	Read			
GetInfrastructureSuggestion [permission only]	Get infrastructure suggestion	Read			
GetIpAddress [permission only]	Get customer's ip address	Read			
GetResourceCostEstimate [permission only]	Get resource cost estimate	Read			
ListProvisionedApps	List provisioning applications	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
[permission only]					
StartProvisioning [permission only]	Start a provisioning	Write			

Resource types defined by Launch Wizard

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

Condition keys for Launch Wizard

Launch Wizard 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 [Available keys for conditions](#).

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 \(p. 1178\)](#)
- [Resource types defined by Amazon Lex \(p. 1183\)](#)
- [Condition keys for Amazon Lex \(p. 1183\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources (“`*`”) in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1183)		
CreateIntentVersion	Creates a new version based on the \$LATEST version of the specified intent	Write	intent version* (p. 1183)		
CreateSlotTypeVersion	Creates a new version based on the \$LATEST version of the specified slot type	Write	slottype version* (p. 1183)		
DeleteBot	Deletes all versions of a bot	Write	bot version* (p. 1183)		
DeleteBotAlias	Deletes an alias for a specific bot	Write	bot alias* (p. 1183)		
DeleteBotChannelAssociation	Deletes the association between Amazon Lex bot alias and a messaging platform	Write	channel* (p. 1183)		
DeleteBotVersion	Deletes a specific version of a bot	Write	bot version* (p. 1183)		
DeleteIntent	Deletes all versions of an intent	Write	intent version* (p. 1183)		
DeleteIntentVersion	Deletes a specific version of an intent	Write	intent version* (p. 1183)		
DeleteSession	Removes session information for a specified bot, alias, and user ID	Write	bot alias (p. 1183) bot version (p. 1183)		
DeleteSlotType	Deletes all versions of a slot type	Write	slottype version* (p. 1183)		
DeleteSlotTypeVersion	Deletes a specific version of a slot type	Write	slottype version* (p. 1183)		
DeleteUtterances	Deletes the information Amazon Lex maintains for utterances on a specific bot and userId	Write	bot version* (p. 1183)		
GetBot	Returns information for a specific bot. In addition to the bot name, the bot version or alias is required	Read	bot alias (p. 1183)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			bot version (p. 1183)		
GetBotAlias	Returns information about a Amazon Lex bot alias	Read	bot alias* (p. 1183)		
GetBotAliases	Returns a list of aliases for a given Amazon Lex bot	List			
GetBotChannelAssociations	Returns information about the association between a Amazon Lex bot and a messaging platform	Read	channel* (p. 1183)		
GetBotChannelAssociations	Returns a list of all of the channels associated with a single bot	List	channel* (p. 1183)		
GetBotVersions	Returns information for all versions of a specific bot	List	bot version* (p. 1183)		
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			
GetExport	Exports Amazon Lex Resource in a requested format	Read	bot version* (p. 1183)		
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* (p. 1183)		
GetIntentVersions	Returns information for all versions of a specific intent	List	intent version* (p. 1183)		
GetIntents	Returns information for the \$LATEST version of all intents, subject to filters provided by the client	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 (p. 1183)		
			bot version (p. 1183)		
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* (p. 1183)		
GetSlotTypeVersions	Returns information for all versions of a specific slot type	List	slottype version* (p. 1183)		
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* (p. 1183)		
ListTagsForResource	Lists tags for a Lex resource	Read	bot (p. 1183)		
			bot alias (p. 1183)		
			channel (p. 1183)		
PostContent	Sends user input (text or speech) to Amazon Lex	Write	bot alias (p. 1183)		
			bot version (p. 1183)		
PostText	Sends user input (text-only) to Amazon Lex	Write	bot alias (p. 1183)		
			bot version (p. 1183)		
PutBot	Creates or updates the \$LATEST version of a Amazon Lex conversational bot	Write	bot version* (p. 1183)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys (p. 1183) aws:RequestTag/\${TagKey} (p. 1183)	
PutBotAlias	Creates or updates an alias for the specific bot	Write	bot alias* (p. 1183)		
				aws:TagKeys (p. 1183) aws:RequestTag/\${TagKey} (p. 1183)	
PutIntent	Creates or updates the \$LATEST version of an intent	Write	intent version* (p. 1183)		
PutSession	Creates a new session or modifies an existing session with an Amazon Lex bot	Write	bot alias (p. 1183)		
			bot version (p. 1183)		
PutSlotType	Creates or updates the \$LATEST version of a slot type	Write	slottype version* (p. 1183)		
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* (p. 1183)		
TagResource	Adds or overwrites tags to a Lex resource	Tagging	bot (p. 1183)		
			bot alias (p. 1183)		
			channel (p. 1183)		
			aws:TagKeys (p. 1183) aws:RequestTag/\${TagKey} (p. 1183)		
UntagResource	Removes tags from a Lex resource	Tagging	bot (p. 1183)		
			bot alias (p. 1183)		
			channel (p. 1183)		
			aws:TagKeys (p. 1183) aws:RequestTag/\${TagKey} (p. 1183)		

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 \(p. 1178\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1183)
bot version	arn:\${Partition}:lex:\${Region}: \${Account}:bot:\${BotName}:\${BotVersion}	aws:ResourceTag/ \${TagKey} (p. 1183)
bot alias	arn:\${Partition}:lex:\${Region}: \${Account}:bot:\${BotName}:\${BotAlias}	aws:ResourceTag/ \${TagKey} (p. 1183)
channel	arn:\${Partition}:lex:\${Region}: \${Account}:bot-channel:\${BotName}: \${BotAlias}:\${ChannelName}	aws:ResourceTag/ \${TagKey} (p. 1183)
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 [Available global condition 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	String
lex:associatedSlotTypes	Enables you to control access based on the slot types included in the request	String

Condition keys	Description	Type
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 \(p. 1184\)](#)
- [Resource types defined by Amazon Lex V2 \(p. 1191\)](#)
- [Condition keys for Amazon Lex V2 \(p. 1192\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BuildBotLocale	Grants permission to build an existing bot locale in a bot	Write	bot* (p. 1191)		
CreateBot	Grants permission to create a new bot and a test bot alias pointing to the DRAFT bot version	Write	bot* (p. 1191) bot alias* (p. 1191)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys (p. 1192) aws:RequestTag/\${TagKey} (p. 1192)	
CreateBotAlias	Grants permission to create a new bot alias in a bot	Write	bot alias* (p. 1191)		
				aws:TagKeys (p. 1192) aws:RequestTag/\${TagKey} (p. 1192)	
CreateBotChannel [permission only]	Grants permission to create a bot channel in an existing bot	Write	bot* (p. 1191)		
CreateBotLocale	Grants permission to create a new bot locale in an existing bot	Write	bot* (p. 1191)		
CreateBotVersion	Grants permission to create a new version of an existing bot	Write	bot* (p. 1191)		
CreateCustomVocabulary [permission only]	Grants permission to create a new custom vocabulary in an existing bot locale	Write	bot* (p. 1191)		
CreateExport	Grants permission to create an export for an existing resource	Write	bot* (p. 1191)		
CreateIntent	Grants permission to create a new intent in an existing bot locale	Write	bot* (p. 1191)		
CreateResourcePolicy	Grants permission to create a new resource policy for a Lex resource	Write	bot (p. 1191)		
bot alias (p. 1191)					
CreateSlot	Grants permission to create a new slot in an intent	Write	bot* (p. 1191)		
CreateSlotType	Grants permission to create a new slot type in an existing bot locale	Write	bot* (p. 1191)		
CreateUploadUrl	Grants permission to create an upload url for import file	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteBot	Grants permission to delete an existing bot	Write	bot* (p. 1191)		lex>DeleteBotAlias lex>DeleteBotChannel lex>DeleteBotLocale lex>DeleteBotVersion lex>DeleteIntent lex>DeleteSlot lex>DeleteSlotType
DeleteBotAlias	Grants permission to delete an existing bot alias in a bot	Write	bot alias* (p. 1191)		
DeleteBotChannel [permission only]	Grants permission to delete an existing bot channel	Write	bot* (p. 1191)		
DeleteBotLocale	Grants permission to delete an existing bot locale in a bot	Write	bot* (p. 1191)		lex>DeleteIntent lex>DeleteSlot lex>DeleteSlotType
DeleteBotVersion	Grants permission to delete an existing bot version	Write	bot* (p. 1191)		
DeleteCustomVocabulary	Grants permission to delete an existing custom vocabulary in a bot locale	Write	bot* (p. 1191)		
DeleteExport	Grants permission to delete an existing export	Write	bot* (p. 1191)		
DeleteImport	Grants permission to delete an existing import	Write	bot* (p. 1191)		
DeleteIntent	Grants permission to delete an existing intent in a bot locale	Write	bot* (p. 1191)		
DeleteResourcePolicy	Grants permission to delete an existing resource policy for a Lex resource	Write	bot (p. 1191)		
bot alias (p. 1191)					
DeleteSession	Grants permission to delete session information for a bot alias and user ID	Write	bot alias* (p. 1191)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteSlot	Grants permission to delete an existing slot in an intent	Write	bot* (p. 1191)		
DeleteSlotType	Grants permission to delete an existing slot type in a bot locale	Write	bot* (p. 1191)		
DeleteUtterances	Grants permission to delete utterance data for a bot	Write	bot* (p. 1191)		
DescribeBot	Grants permission to retrieve an existing bot	Read	bot* (p. 1191)		
DescribeBotAlias	Grants permission to retrieve an existing bot alias	Read	bot alias* (p. 1191)		
DescribeBotChannel [permission only]	Grants permission to retrieve an existing bot channel	Read	bot* (p. 1191)		
DescribeBotLocale	Grants permission to retrieve an existing bot locale	Read	bot* (p. 1191)		
DescribeBotRecommendation	Grants permission to retrieve metadata information about a bot recommendation	Read	bot* (p. 1191)		
DescribeBotVersion	Grants permission to retrieve an existing bot version	Read	bot* (p. 1191)		
DescribeCustomVocabulary [permission only]	Grants permission to retrieve an existing custom vocabulary	Read	bot* (p. 1191)		
DescribeCustomVocabulary	Grants permission to retrieve metadata of an existing custom vocabulary	Read	bot* (p. 1191)		
DescribeExport	Grants permission to retrieve an existing export	Read	bot* (p. 1191)		lex:DescribeBot lex:DescribeBotLocale lex:DescribeIntent lex:DescribeSlot lex:DescribeSlotType lex>ListBotLocales lex>ListIntents lex>ListSlotTypes lex>ListSlots

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeImport	Grants permission to retrieve an existing import	Read	bot* (p. 1191)		
DescribeIntent	Grants permission to retrieve an existing intent	Read	bot* (p. 1191)		
DescribeResourcePolicy <small>[permission only]</small>	Grants permission to retrieve an existing resource policy for a Lex resource	Read	bot (p. 1191)		
			bot alias (p. 1191)		
DescribeSlot	Grants permission to retrieve an existing slot	Read	bot* (p. 1191)		
DescribeSlotType	Grants permission to retrieve an existing slot type	Read	bot* (p. 1191)		
GetSession	Grants permission to retrieve session information for a bot alias and user ID	Read	bot alias* (p. 1191)		
ListAggregatedUtterances	Grants permission to list utterances and statistics for a bot	List	bot* (p. 1191)		
ListBotAliases	Grants permission to list bot aliases in a bot	List	bot* (p. 1191)		
ListBotChannels <small>[permission only]</small>	Grants permission to list bot channels	List	bot* (p. 1191)		
ListBotLocales	Grants permission to list bot locales in a bot	List	bot* (p. 1191)		
ListBotRecommendations	Grants permission to get a list of bot recommendations that meet the specified criteria	List	bot* (p. 1191)		
ListBotVersions	Grants permission to list existing bot versions	List	bot* (p. 1191)		
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			
ListExports	Grants permission to list existing exports	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListImports	Grants permission to list existing imports	List			
ListIntents	Grants permission to list intents in a bot	List	bot* (p. 1191)		
ListRecommendedIntents	Grants permission to get a list of recommended intents provided by the bot recommendation	List	bot* (p. 1191)		
ListSlotTypes	Grants permission to list slot types in a bot	List	bot* (p. 1191)		
ListSlots	Grants permission to list slots in an intent	List	bot* (p. 1191)		
ListTagsForResource	Grants permission to lists tags for a Lex resource	Read	bot (p. 1191) bot alias (p. 1191)		
PutSession	Grants permission to create a new session or modify an existing session for a bot alias and user ID	Write	bot alias* (p. 1191)		
RecognizeText	Grants permission to send user input (text-only) to an bot alias	Write	bot alias* (p. 1191)		
RecognizeUtterance	Grants permission to send user input (text or speech) to an bot alias	Write	bot alias* (p. 1191)		
SearchAssociatedTranscripts	Grants permission to search for associated transcripts that meet the specified criteria	List	bot* (p. 1191)		
StartBotRecommendation	Grants permission to start a bot recommendation for an existing bot locale	Write	bot* (p. 1191)		
StartConversation	Grants permission to stream user input (speech/text/DTMF) to a bot alias	Write	bot alias* (p. 1191)		

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 (p. 1191)		lex>CreateBot lex>CreateBotLocale lex>CreateIntent lex>CreateSlot lex>CreateSlotType lex>DeleteBotLocale lex>DeleteIntent lex>DeleteSlot lex>DeleteSlotType lex>UpdateBot lex>UpdateBotLocale lex>UpdateIntent lex>UpdateSlot lex>UpdateSlotType
				bot alias (p. 1191)	
TagResource	Grants permission to add or overwrite tags of a Lex resource	Tagging	bot (p. 1191)		
			bot alias (p. 1191)		
				aws:TagKeys (p. 1192) aws:RequestTag/\${TagKey} (p. 1192)	
UntagResource	Grants permission to remove tags from a Lex resource	Tagging	bot (p. 1191)		
			bot alias (p. 1191)		
				aws:TagKeys (p. 1192) aws:RequestTag/\${TagKey} (p. 1192)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateBot	Grants permission to update an existing bot	Write	bot* (p. 1191)		
UpdateBotAlias	Grants permission to update an existing bot alias	Write	bot alias* (p. 1191)		
UpdateBotLocale	Grants permission to update an existing bot locale	Write	bot* (p. 1191)		
UpdateBotRecommendation	Grants permission to update an existing bot recommendation request	Write	bot* (p. 1191)		
UpdateCustomVocabulary [permission only]	Grants permission to update an existing custom vocabulary	Write	bot* (p. 1191)		
UpdateExport	Grants permission to update an existing export	Write	bot* (p. 1191)		
UpdateIntent	Grants permission to update an existing intent	Write	bot* (p. 1191)		
UpdateResourcePolicy	Grants permission to update an existing resource policy for a Lex resource	Write	bot (p. 1191)	bot alias (p. 1191)	
UpdateSlot	Grants permission to update an existing slot	Write	bot* (p. 1191)		
UpdateSlotType	Grants permission to update an existing slot type	Write	bot* (p. 1191)		

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 \(p. 1184\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
bot	<code>arn:\${Partition}:lex:\${Region}: \${Account}:bot/\${BotId}</code>	aws:ResourceTag/\${TagKey} (p. 1192)
bot alias	<code>arn:\${Partition}:lex:\${Region}: \${Account}:bot-alias/\${BotId}/\${BotAliasId}</code>	aws:ResourceTag/\${TagKey} (p. 1192)

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters access by the tags in the request	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters access by the tags attached to a Lex resource	String
<code>aws:TagKeys</code>	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 keys for use in IAM permission policies.

References:

- Learn how to [configure this service](#).
- View a list of the [API 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 \(p. 1192\)](#)
- [Resource types defined by AWS License Manager \(p. 1195\)](#)
- [Condition keys for AWS License Manager \(p. 1196\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1196)		
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* (p. 1196)		
CheckoutLicense	Grants permission to check out license entitlements	Write			
CreateGrant	Grants permission to create a new grant for license	Write	license* (p. 1196)		
CreateGrantVersion	Grants permission to create new version of grant	Write	grant* (p. 1196)		
CreateLicense	Grants permission to create a new license	Write			
CreateLicenseConfiguration	Grants permission to create a new license configuration	Write		aws:RequestTag/\${TagKey} (p. 1196) aws:TagKeys (p. 1196)	
CreateLicenseConversionTask	Grants permission to create a license conversion task for a resource	Write			
CreateLicenseManagerReportGenerator	Grants permission to create a report generator for a license configuration	Write		aws:RequestTag/\${TagKey} (p. 1196) aws:TagKeys (p. 1196)	
CreateLicenseVersion	Grants permission to create new version of license	Write	license* (p. 1196)		
CreateToken	Grants permission to create a new token for license	Write	license* (p. 1196)		
DeleteGrant	Grants permission to delete a grant	Write	grant* (p. 1196)		
DeleteLicense	Grants permission to delete a license	Write	license* (p. 1196)		
DeleteLicenseConfiguration	Grants permission to permanently delete a license configuration	Write	license-configuration* (p. 1196)		

Service Authorization Reference
Service Authorization Reference
AWS License Manager

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteLicenseManagerReportGenerator	Grants permission to delete a report generator	Write	report-generator* (p. 1196)		
DeleteToken	Grants permission to delete token	Write			
ExtendLicenseConsumption	Grants permission to extend consumption period of already checkout license entitlements	Write			
GetAccessToken	Grants permission to get access token	Read			
GetGrant	Grants permission to get a grant	Read	grant* (p. 1196)		
GetLicense	Grants permission to get a license	Read	license* (p. 1196)		
GetLicenseConfig	Grants permission to get a license configuration	Read	license-configuration* (p. 1196)		
GetLicenseConversionTask	Grants permission to retrieve a license conversion task	Read			
GetLicenseManagerReportGenerator	Grants permission to get a report generator	Read	report-generator* (p. 1196)		
GetLicenseUsage	Grants permission to get a license usage	Read	license* (p. 1196)		
GetServiceSettings	Grants permission to get service settings	List			
ListAssociationsForLicenseConfiguration	Grants permission to list associations for a selected license configuration	List	license-configuration* (p. 1196)		
ListDistributedGrants	Grants permission to list distributed grants	List			
ListFailuresForLicenseConfigurationOperations	Grants permission to list the license configuration operations that failed	List	license-configuration* (p. 1196)		
ListLicenseConfigurations	Grants permission to list license configurations	Read			
ListLicenseConversionTasks	Grants permission to list license conversion tasks	List			
ListLicenseManagerReportGenerators	Grants permission to list report generators	List	license-configuration (p. 1196)		
ListLicenseSpecificationsForResource	Grants permission to list license specifications associated with a selected resource	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListLicenseVersion	Grants permission to list license versions	List	license* (p. 1196)		
ListLicenses	Grants permission to list licenses	Read			
ListReceivedGrant	Grants permission to list received grants	List			
ListReceivedLicen	Grants permission to list received licenses	List			
ListResourceInven	Grants permission to list resource inventory	List			
ListTagsForResour	Grants permission to list tags for a selected resource	Read	license-configuration* (p. 1196)		
ListTokens	Grants permission to list tokens	List			
ListUsageForLicen	Grants permission to list usage records for a selected license configuration	List	license-configuration* (p. 1196)		
RejectGrant	Grants permission to reject a grant	Write	grant* (p. 1196)		
TagResource	Grants permission to tag a selected resource	Tagging	license-configuration* (p. 1196)		
			aws:RequestTag/\${TagKey} (p. 1196)		
			aws:TagKeys (p. 1196)		
UntagResource	Grants permission to untag a selected resource	Tagging	license-configuration* (p. 1196)		
UpdateLicenseConfi	Grants permission to update an existing license configuration	Write	license-configuration* (p. 1196)		
UpdateLicenseMatri	Grants permission to update a report generator for a license configuration	Write	report-generator* (p. 1196)		
UpdateLicenseSpecifi	Grants permission to update license specifications for a selected resource	Write	license-configuration* (p. 1196)		
UpdateServiceSetti	Grants permission to update 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](#) (p. 1192) identifies the resource

types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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}	license-manager:ResourceTag/\${TagKey} (p. 1196)
license	arn:\${Partition}:license-manager::\${Account}:license:\${LicenseId}	
grant	arn:\${Partition}:license-manager::\${Account}:grant:\${GrantId}	
report-generator	arn:\${Partition}:license-manager:\${Region}:\${Account}:report-generator:\${ReportGeneratorId}	license-manager:ResourceTag/\${TagKey} (p. 1196)

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 [Available global condition 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 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 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 \(p. 1197\)](#)
- [Resource types defined by Amazon Lightsail \(p. 1211\)](#)
- [Condition keys for Amazon Lightsail \(p. 1212\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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	StaticIp* (p. 1212)		
AttachCertificate	Grants permission to attach an SSL/TLS certificate to your Amazon Lightsail content delivery network (CDN) distribution	Write	Certificate* (p. 1212)		
			Distribution* (p. 1212)		
AttachDisk	Grants permission to attach a disk to an instance	Write	Disk* (p. 1212)		
			Instance* (p. 1211)		
AttachInstancesToLoadBalancer	Grants permission to attach one or more instances to a load balancer	Write	Instance* (p. 1211)		
			LoadBalancer* (p. 1212)		
AttachLoadBalancerTLSCertificate	Grants permission to attach a TLS certificate to a load balancer	Write	LoadBalancer* (p. 1212)		
AttachStaticIp	Grants permission to attach a static IP address to an instance	Write	Instance* (p. 1211)		
			StaticIp* (p. 1212)		
CloseInstancePublicPort	Grants permission to close a public port of an instance	Write	Instance* (p. 1211)		
CopySnapshot	Grants permission to copy a snapshot from one AWS Region to another in Amazon Lightsail	Write	DiskSnapshot (p. 1212)		
			InstanceSnapshot (p. 1211)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateBucket	Grants permission to create an Amazon Lightsail bucket	Write	Bucket* (p. 1212)		
			aws:RequestTag/ {\$TagKey} (p. 1213)	aws:TagKeys (p. 1213)	
CreateBucketAccessKey	Grants permission to create a new access key for the specified bucket	Write	Bucket* (p. 1212)		
CreateCertificate	Grants permission to create an SSL/TLS certificate	Write	Certificate* (p. 1212)		
CreateCloudFormationStack	Grants permission to create a new Amazon EC2 instance from an exported Amazon Lightsail snapshot	Write	ExportSnapshotRecord* (p. 1212)		
CreateContactMethod	Grants permission to create email or SMS text message contact method	Write			
CreateContainerService	Grants permission to create an Amazon Lightsail container service	Write	ContainerService* (p. 1212)		
CreateContainerServiceDeployment	Grants permission to create a deployment for your Amazon Lightsail container service	Write	ContainerService* (p. 1212)		
CreateContainerServiceTemporaryPort	Grants permission to create a temporary port for 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	Disk* (p. 1212)		
			aws:RequestTag/ {\$TagKey} (p. 1213)	aws:TagKeys (p. 1213)	
CreateDiskFromSnapshot	Grants permission to create a disk from snapshot	Write	Disk* (p. 1212)		
			aws:RequestTag/ {\$TagKey} (p. 1213)	aws:TagKeys (p. 1213)	
CreateDiskSnapshot	Grants permission to create a disk snapshot	Write	Disk* (p. 1212)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 1213) aws:TagKeys (p. 1213)	
CreateDistribution	Grants permission to create an Amazon Lightsail content delivery network (CDN) distribution	Write	Distribution* (p. 1212)		
CreateDomain	Grants permission to create a domain resource for the specified domain name	Write	Domain* (p. 1211)		
				aws:RequestTag/ \${TagKey} (p. 1213) aws:TagKeys (p. 1213)	
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* (p. 1211)		
CreateInstanceSnapshot	Grants permission to create an instance snapshot	Write	Instance* (p. 1211)		
			InstanceSnapshot* (p. 1211)		
				aws:RequestTag/ \${TagKey} (p. 1213)	
				aws:TagKeys (p. 1213)	
CreateInstances	Grants permission to create one or more instances	Write	KeyValuePair* (p. 1212)		
				aws:RequestTag/ \${TagKey} (p. 1213)	
				aws:TagKeys (p. 1213)	
CreateInstancesFromSnapshot	Grants permission to create one or more instances based on an instance snapshot	Write	Instance* (p. 1211)		
			InstanceSnapshot* (p. 1211)		
				aws:RequestTag/ \${TagKey} (p. 1213)	
				aws:TagKeys (p. 1213)	
CreateKeyPair	Grants permission to create a key pair used to authenticate and connect to an instance	Write	KeyValuePair* (p. 1212)		
				aws:RequestTag/ \${TagKey} (p. 1213)	
				aws:TagKeys (p. 1213)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLoadBalancer	Grants permission to create a load balancer	Write	LoadBalancer* (p. 1212)		
	aws:RequestTag/ \${TagKey} (p. 1213)				
	aws:TagKeys (p. 1213)				
CreateLoadBalancerTLScertificate	Grants permission to create a Load Balancer TLS certificate	Write	LoadBalancer* (p. 1212)		
CreateRelationalDatabase	Grants permission to create a new relational database	Write	RelationalDatabase* (p. 1212)		
aws:RequestTag/ \${TagKey} (p. 1213)					
aws:TagKeys (p. 1213)					
CreateRelationalDatabaseSnapshot	Grants permission to create a new relational database from a snapshot	Write	RelationalDatabase* (p. 1212)		
aws:RequestTag/ \${TagKey} (p. 1213)					
aws:TagKeys (p. 1213)					
CreateRelationalDatabaseSnapshot	Grants permission to create a relational database snapshot	Write	RelationalDatabaseSnapshot* (p. 1212)		
aws:RequestTag/ \${TagKey} (p. 1213)					
aws:TagKeys (p. 1213)					
DeleteAlarm	Grants permission to delete an alarm	Write	Alarm* (p. 1212)		
DeleteAutoSnapshot	Grants permission to delete an automatic snapshot of an instance or disk	Write	Disk (p. 1212)		
Instance (p. 1211)					
DeleteBucket	Grants permission to delete an Amazon Lightsail bucket	Write	Bucket* (p. 1212)		
DeleteBucketAccessKey	Grants permission to delete an access key for the specified Amazon Lightsail bucket	Write	Bucket* (p. 1212)		
DeleteCertificate	Grants permission to delete an SSL/TLS certificate	Write	Certificate* (p. 1212)		
DeleteContactMethod	Grants permission to delete a contact method	Write	ContactMethod* (p. 1212)		
DeleteContainerImage	Grants permission to delete a container image that is registered to your Amazon Lightsail container service	Write	ContainerService* (p. 1212)		

Service Authorization Reference
Service Authorization Reference
Amazon Lightsail

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteContainerService	Grants permission to delete your Amazon Lightsail container service	Write	ContainerService* (p. 1212)		
DeleteDisk	Grants permission to delete a disk	Write	Disk* (p. 1212)		
DeleteDiskSnapshot	Grants permission to delete a disk snapshot	Write	Disk* (p. 1212)		
DeleteDistribution	Grants permission to delete your Amazon Lightsail content delivery network (CDN) distribution	Write	Distribution* (p. 1212)		
DeleteDomain	Grants permission to delete a domain resource and all of its DNS records	Write	Domain* (p. 1211)		
DeleteDomainEntry	Grants permission to delete a DNS record entry for a domain resource	Write	Domain* (p. 1211)		
DeleteInstance	Grants permission to delete an instance	Write	Instance* (p. 1211)		
DeleteInstanceSnapshot	Grants permission to delete an instance snapshot	Write	InstanceSnapshot* (p. 1211)		
DeleteKeyPair	Grants permission to delete a key pair used to authenticate and connect to an instance	Write	KeyPair* (p. 1212)		
DeleteKnownHostKey	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* (p. 1211)		
DeleteLoadBalancer	Grants permission to delete a load balancer	Write	LoadBalancer* (p. 1212)		
DeleteLoadBalancerTLSCertificate	Grants permission to delete a load balancer TLS certificate	Write	LoadBalancer* (p. 1212)		
DeleteRelationalDatabase	Grants permission to delete a relational database	Write	RelationalDatabase* (p. 1212)		
DeleteRelationalDatabaseSnapshot	Grants permission to delete a relational database snapshot	Write	RelationalDatabaseSnapshot* (p. 1212)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DetachCertificateFromSSLDistribution	Grants permission to detach an SSL/TLS certificate from your Amazon Lightsail content delivery network (CDN) distribution	Write	Distribution* (p. 1212)		
DetachDisk	Grants permission to detach a disk from an instance	Write	Disk* (p. 1212)		
DetachInstancesFromLoadBalancer	Grants permission to detach one or more instances from a load balancer	Write	Instance* (p. 1211)		
			LoadBalancer* (p. 1212)		
DetachStaticIp	Grants permission to detach a static IP from an instance to which it is attached	Write	Instance* (p. 1211)		
DisableAddOn	Grants permission to disable an add-on for an Amazon Lightsail resource	Write	Disk (p. 1212)		
			Instance (p. 1211)		
DownloadDefaultKeyPair	Grants permission to download the default key pair used to authenticate and connect to instances in a specific AWS Region	Write	KeyPair* (p. 1212)		
EnableAddOn	Grants permission to enable or modify an add-on for an Amazon Lightsail resource	Write	Disk (p. 1212)		
			Instance (p. 1211)		
ExportSnapshot	Grants permission to export an Amazon Lightsail snapshot to Amazon EC2	Write			
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			
GetAutoSnapshot	Grants permission to view the available automatic snapshots for an instance or disk	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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			
GetCloudFormationInformation	Grants permission to get information about all CloudFormation stacks used to create Amazon EC2 resources from exported Amazon Lightsail snapshots	Read	CloudFormationStackRecord* (p. 1212)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetContactMethods	Grants permission to view information about the configured contact methods	Read			
GetContainerAPINodeInformation	Grants permission to view information about Amazon Lightsail containers, such as the current version of the Lightsail Control (lightsailctl) plugin	Read			
GetContainerImageList	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			
GetContainerServiceMetricsDataPoints	Grants permission to view the Data Points of a specific metric of your Amazon Lightsail container service	Read			
GetContainerServicePowersList	Grants permission to view the List of powers that can be specified for your Amazon Lightsail container services	Read			
GetContainerServicesList	Grants permission to view information about one or more of your Amazon Lightsail container services	Read			
GetDisk	Grants permission to get information about a disk	Read	Disk* (p. 1212)		
GetDiskSnapshot	Grants permission to get information about a disk snapshot	Read	Disk* (p. 1212)		
GetDiskSnapshotList	Grants permission to get information about all disk snapshots	Read	Disk* (p. 1212)		
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 your Amazon Lightsail content delivery network (CDN) distributions	Read			
GetDistributionLastResetTime	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	Domain* (p. 1211)		
GetDomains	Grants permission to get DNS records for all domain resources	Read	Domain* (p. 1211)		
GetExportSnapshotInformation	Grants permission to get information about all records of exported Amazon Lightsail snapshots to Amazon EC2	Read	ExportSnapshotRecord* (p. 1212)		
GetInstance	Grants permission to get information about an instance	Read	Instance* (p. 1211)		
GetInstanceAccessTemporaryKeys	Grants permission to get temporary keys you can use to authenticate and connect to an instance	Write	Instance* (p. 1211)		
GetInstanceMetricData	Grants permission to get the data points for the specified metric of an instance	Read	Instance* (p. 1211)		
GetInstancePortStates	Grants permission to get the port states of an instance	Read	Instance* (p. 1211)		
GetInstanceSnapshotInformation	Grants permission to get information about an instance snapshot	Read	InstanceSnapshot* (p. 1211)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetInstanceSnapshots	Grants permission to get information about all instance snapshots	Read	InstanceSnapshot* (p. 1211)		
GetInstanceState	Grants permission to get the state of an instance	Read	Instance* (p. 1211)		
GetInstances	Grants permission to get information about all instances	Read	Instance* (p. 1211)		
GetKeyPair	Grants permission to get information about a key pair	Read	KeyValuePair* (p. 1212)		
GetKeyPairs	Grants permission to get information about all key pairs	Read	KeyValuePair* (p. 1212)		
GetLoadBalancer	Grants permission to get information about a load balancer	Read	LoadBalancer* (p. 1212)		
GetLoadBalancerDataPoints	Grants permission to get the DataPoints for the specified metric of a load balancer	Read	LoadBalancer* (p. 1212)		
GetLoadBalancerInformation	Grants permission to get Information about a load balancer's TLS certificates	Read	LoadBalancer* (p. 1212)		
GetLoadBalancers	Grants permission to get information about load balancers	Read	LoadBalancer* (p. 1212)		
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	Domain (p. 1211)		
Instance (p. 1211)					
InstanceSnapshot (p. 1211)					
KeyValuePair (p. 1212)					
StaticIp (p. 1212)					

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRegions	Grants permission to get a list of all valid AWS Regions for Amazon Lightsail	Read			
GetRelationalDatabaseBlueprints	Grants permission to get information about a relational database	Read	RelationalDatabase* (p. 1212)		
GetRelationalDatabaseBundles	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			
GetRelationalDatabaseEvents	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			
GetRelationalDatabaseLogStreams	Grants permission to get events for a relational database	Read			
GetRelationalDatabaseLogStream	Grants permission to get events for the specified log stream of a relational database	Read			
GetRelationalDatabaseStreamsAvailable	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			
GetRelationalDatabaseMetrics	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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRelationalDatabaseInformation	Grants permission to get information about a relational database snapshot	Read	RelationalDatabase* (p. 1212)		
GetRelationalDatabaseInformation	Grants permission to get information about all relational database snapshots	Read	RelationalDatabase* (p. 1212)		
GetRelationalDatabaseInformation	Grants permission to get information about all relational databases	Read	RelationalDatabase* (p. 1212)		
GetStaticIp	Grants permission to get information about a static IP	Read	StaticIp* (p. 1212)		
GetStaticIps	Grants permission to get information about all static IPs	Read	StaticIp* (p. 1212)		
ImportKeyPair	Grants permission to import a public key from a key pair	Write	KeyValuePair* (p. 1212)		
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* (p. 1211)		
PeerVpc	Grants permission to try to peer the Amazon Lightsail virtual private cloud (VPC) with the default VPC	Write			
PutAlarm	Grants permission to creates or update an alarm, and associate it with the specified metric	Write	Alarm* (p. 1212)		
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* (p. 1211)		
RebootInstance	Grants permission to reboot an instance that is in a running state	Write	Instance* (p. 1211)		
RebootRelationalDatabase	Grants permission to reboot a relational database that is in a running state	Write	RelationalDatabase* (p. 1212)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterContainerImage	Grants permission to register a container image to your Amazon Lightsail container service	Write	ContainerService* (p. 1212)		
ReleaseStaticIp	Grants permission to delete a static IP	Write	StaticIp* (p. 1212)		
ResetDistribution	Grants permission to delete currently cached content from your Amazon Lightsail content delivery network (CDN) distribution	Write	Distribution* (p. 1212)		
SendContactMethodVerification	Grants permission to send a verification request to an email contact method to ensure it's owned by the requester	Write	ContactMethod* (p. 1212)		
SetIpAddressType	Grants permission to set the IP address type for a Amazon Lightsail resource	Write	Distribution (p. 1212)		
			Instance (p. 1211)		
			LoadBalancer (p. 1212)		
SetResourceAccess	Grants permission to set the Amazon Lightsail resources that can access the specified Amazon Lightsail bucket	Write	Bucket* (p. 1212)		
StartInstance	Grants permission to start an instance that is in a stopped state	Write	Instance* (p. 1211)		
StartRelationalDatabase	Grants permission to start a relational database that is in a stopped state	Write	RelationalDatabase* (p. 1212)		
StopInstance	Grants permission to stop an instance that is in a running state	Write	Instance* (p. 1211)		
StopRelationalDatabase	Grants permission to stop a relational database that is in a running state	Write	RelationalDatabase* (p. 1212)		
TagResource	Grants permission to tag a resource	Tagging	Disk (p. 1212)		
			DiskSnapshot (p. 1212)		
			Domain (p. 1211)		
			Instance (p. 1211)		
			InstanceSnapshot (p. 1211)		
			KeyValuePair (p. 1212)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			LoadBalancer (p. 1212) RelationalDatabase (p. 1212) RelationalDatabaseSnapshot (p. 1212) StaticIp (p. 1212)	aws:RequestTag/\${TagKey} (p. 1213) aws:TagKeys (p. 1213)	
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* (p. 1212)		
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	Disk (p. 1212)		
			DiskSnapshot (p. 1212)		
			Domain (p. 1211)		
			Instance (p. 1211)		
			InstanceSnapshot (p. 1211)		
			KeyPair (p. 1212)		
			LoadBalancer (p. 1212)		
			RelationalDatabase (p. 1212)		
			RelationalDatabaseSnapshot (p. 1212)		
			StaticIp (p. 1212)		
UpdateBucket	Grants permission to update an existing Amazon Lightsail bucket	Write	Bucket* (p. 1212)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateContainerServiceConfiguration	Grants permission to update the configuration of your Amazon Lightsail container service, such as its power, scale, and public domain names	Write	ContainerService* (p. 1212)		
UpdateDistribution	Grants permission to update an existing Amazon Lightsail content delivery network (CDN) distribution or its configuration	Write	Distribution* (p. 1212)		
UpdateDistributionBundle	Grants permission to update the bundle of your Amazon Lightsail content delivery network (CDN) distribution	Write	Distribution* (p. 1212)		
UpdateDomainEntry	Grants permission to update a domain recordset after it is created	Write	Domain* (p. 1211)		
UpdateLoadBalancer	Grants permission to update a load balancer attribute, such as the health check path and session stickiness	Write	LoadBalancer* (p. 1212)		
UpdateRelationalDatabase	Grants permission to update a relational database	Write	RelationalDatabase* (p. 1212)		
UpdateRelationalDatabaseParameters	Grants permission to update the parameters of a relational database	Write			

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 \(p. 1197\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1213)
Instance	arn:\${Partition}:lightsail:\${Region}: \${Account}:Instance/\${Id}	aws:ResourceTag/ \${TagKey} (p. 1213)
InstanceSnapshot	arn:\${Partition}:lightsail:\${Region}: \${Account}:InstanceSnapshot/\${Id}	aws:ResourceTag/ \${TagKey} (p. 1213)

Resource types	ARN	Condition keys
KeyPair	arn:\${Partition}:lightsail:\${Region}: \${Account}:KeyPair/\${Id}	aws:ResourceTag/ \${TagKey} (p. 1213)
StaticIp	arn:\${Partition}:lightsail:\${Region}: \${Account}:StaticIp/\${Id}	aws:ResourceTag/ \${TagKey} (p. 1213)
Disk	arn:\${Partition}:lightsail:\${Region}: \${Account}:Disk/\${Id}	aws:ResourceTag/ \${TagKey} (p. 1213)
DiskSnapshot	arn:\${Partition}:lightsail:\${Region}: \${Account}:DiskSnapshot/\${Id}	aws:ResourceTag/ \${TagKey} (p. 1213)
LoadBalancer	arn:\${Partition}:lightsail:\${Region}: \${Account}:LoadBalancer/\${Id}	aws:ResourceTag/ \${TagKey} (p. 1213)
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} (p. 1213)
RelationalDatabaseSnapshot	arn:\${Partition}:lightsail:\${Region}: \${Account}:RelationalDatabaseSnapshot/\${Id}	aws:ResourceTag/ \${TagKey} (p. 1213)
Alarm	arn:\${Partition}:lightsail:\${Region}: \${Account}:Alarm/\${Id}	
Certificate	arn:\${Partition}:lightsail:\${Region}: \${Account}:Certificate/\${Id}	
ContactMethod	arn:\${Partition}:lightsail:\${Region}: \${Account}:ContactMethod/\${Id}	
ContainerService	arn:\${Partition}:lightsail:\${Region}: \${Account}:ContainerService/\${Id}	
Distribution	arn:\${Partition}:lightsail:\${Region}: \${Account}:Distribution/\${Id}	
Bucket	arn:\${Partition}:lightsail:\${Region}: \${Account}:Bucket/\${Id}	aws:ResourceTag/ \${TagKey} (p. 1213)

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters actions based on the presence of tag key-value pairs in the request	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters actions based on tag key-value pairs attached to the resource	String
<code>aws:TagKeys</code>	Filters actions based on the presence of tag keys 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 \(p. 1213\)](#)
- [Resource types defined by Amazon Location \(p. 1218\)](#)
- [Condition keys for Amazon Location \(p. 1218\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateTrackerAssociation	Grants permission to create an association between a geofence-collection and a tracker resource	Write	tracker* (p. 1218)		
BatchDeleteDevicePositionHistories	Grants permission to delete a batch of device position histories from a tracker resource	Write	tracker* (p. 1218)		
BatchDeleteGeofences	Grants permission to delete a batch of geofences from a geofence collection	Write	geofence-collection* (p. 1218)		
BatchEvaluateGeofences	Grants permission to evaluate devices positions against the position of geofences in a given geofence collection	Write	geofence-collection* (p. 1218)		
BatchGetDevicePositions	Grants permission to send a batch request to retrieve device positions	Read	tracker* (p. 1218)		
BatchPutGeofences	Grants permission to send a batch request for adding geofences into a given geofence collection	Write	geofence-collection* (p. 1218)		
BatchUpdateDevicePositions	Grants permission to upload a position update for one or more devices to a tracker resource	Write	tracker* (p. 1218)		
CalculateRoute	Grants permission to calculate routes using a given route calculator resource	Read	route-calculator* (p. 1218)		
CalculateRouteMatrix	Grants permission to calculate a route matrix using a given route calculator resource	Read	route-calculator* (p. 1218)		
CreateGeofenceCollection	Grants permission to create a geofence-collection	Write		aws:RequestTag/\${TagKey} (p. 1218) aws:TagKeys (p. 1218)	
CreateMap	Grants permission to create a map resource	Write		aws:RequestTag/\${TagKey} (p. 1218) aws:TagKeys (p. 1218)	
CreatePlaceIndex	Grants permission to create a place index resource	Write		aws:RequestTag/\${TagKey} (p. 1218) aws:TagKeys (p. 1218)	
CreateRouteCalculator	Grants permission to create a route calculator resource	Write		aws:RequestTag/\${TagKey} (p. 1218)	

Service Authorization Reference
Service Authorization Reference
Amazon Location

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					aws:TagKeys (p. 1218)
CreateTracker	Grants permission to create a tracker resource	Write		aws:RequestTag/\${TagKey} (p. 1218) aws:TagKeys (p. 1218)	
DeleteGeofenceCollection	Grants permission to delete a geofence-collection	Write	geofence-collection* (p. 1218)		
DeleteMap	Grants permission to delete a map resource	Write	map* (p. 1218)		
DeletePlaceIndex	Grants permission to delete a place index resource	Write	place-index* (p. 1218)		
DeleteRouteCalculator	Grants permission to delete a route calculator resource	Write	route-calculator* (p. 1218)		
DeleteTracker	Grants permission to delete a tracker resource	Write	tracker* (p. 1218)		
DescribeGeofenceCollection	Grants permission to retrieve geofence-collection details	Read	geofence-collection* (p. 1218)		
DescribeMap	Grants permission to retrieve map resource details	Read	map* (p. 1218)		
DescribePlaceIndex	Grants permission to retrieve place-index resource details	Read	place-index* (p. 1218)		
DescribeRouteCalculator	Grants permission to retrieve route calculator resource details	Read	route-calculator* (p. 1218)		
DescribeTracker	Grants permission to retrieve a tracker resource details	Read	tracker* (p. 1218)		
DisassociateTrackerGeofence	Grants permission to remove the association between a tracker resource and a geofence-collection	Write	tracker* (p. 1218)		
GetDevicePosition	Grants permission to retrieve the latest device position	Read	tracker* (p. 1218)		
GetDevicePositionHistory	Grants permission to retrieve the device position history	Read	tracker* (p. 1218)		
GetGeofence	Grants permission to retrieve the geofence details from a geofence-collection	Read	geofence-collection* (p. 1218)		
GetMapGlyphs	Grants permission to retrieve the glyph file for a map resource	Read	map* (p. 1218)		
GetMapSprites	Grants permission to retrieve the sprite file for a map resource	Read	map* (p. 1218)		

Service Authorization Reference
Service Authorization Reference
Amazon Location

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetMapStyleDescriptor	Grants permission to retrieve the map-style descriptor from a map resource	Read	map* (p. 1218)		
GetMapTile	Grants permission to retrieve the map tile from the map resource	Read	map* (p. 1218)		
ListDevicePosition	Grants permission to retrieve a list of devices and their latest positions from the given tracker resource	Read	tracker* (p. 1218)		
ListGeofenceCollection	Grants permission to lists geofence-collections	List			
ListGeofences	Grants permission to list geofences stored in a given geofence collection	Read	geofence-collection* (p. 1218)		
ListMaps	Grants permission to list map resources	List			
ListPlaceIndexes	Grants permission to return a list of place index resources	List			
ListRouteCalculator	Grants permission to return a list of route calculator resources	List			
ListTagsForResource	Grants permission to list the tags (metadata) which you have assigned to the resource	Read	geofence-collection (p. 1218)		
			map (p. 1218)		
			place-index (p. 1218)		
			route-calculator (p. 1218)		
			tracker (p. 1218)		
ListTrackerConsumer	Grants permission to retrieve a list of geofence collections currently associated to the given tracker resource	Read	tracker* (p. 1218)		
ListTrackers	Grants permission to return a list of tracker resources	List			
PutGeofence	Grants permission to add a new geofence or update an existing geofence to a given geofence-collection	Write	geofence-collection* (p. 1218)		
SearchPlaceIndexForGeopoint	Grants permission to reverse geocode a given coordinate	Read	place-index* (p. 1218)		

Service Authorization Reference
Service Authorization Reference
Amazon Location

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SearchPlaceIndex	Grants permission to generate suggestions for addresses and points of interest based on partial or misspelled free-form text	Read	place-index* (p. 1218)		
SearchPlaceIndex	Grants permission to geocode free-form text, such as an address, name, city or region	Read	place-index* (p. 1218)		
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	geofence-collection (p. 1218)		
			map (p. 1218)		
			place-index (p. 1218)		
			route-calculator (p. 1218)		
			tracker (p. 1218)		
				aws:RequestTag/\${TagKey} (p. 1218)	
				aws:TagKeys (p. 1218)	
UntagResource	Grants permission to remove the given tags (metadata) from the resource	Tagging	geofence-collection (p. 1218)		
			map (p. 1218)		
			place-index (p. 1218)		
			route-calculator (p. 1218)		
			tracker (p. 1218)		
				aws:RequestTag/\${TagKey} (p. 1218)	
				aws:TagKeys (p. 1218)	
UpdateGeofenceCollection	Grants permission to update a geofence collection	Write	geofence-collection* (p. 1218)		
UpdateMap	Grants permission to update a map resource	Write	map* (p. 1218)		
UpdatePlaceIndex	Grants permission to update a place index resource	Write	place-index* (p. 1218)		
UpdateRouteCalculator	Grants permission to update a route calculator resource	Write	route-calculator* (p. 1218)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateTracker	Grants permission to update a tracker resource	Write	tracker* (p. 1218)		

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 \(p. 1213\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
geofence-collection	arn:\${Partition}:geo:\${Region}: \${Account}:geofence-collection/ \${GeofenceCollectionName}	aws:ResourceTag/\${TagKey} (p. 1218)
map	arn:\${Partition}:geo:\${Region}: \${Account}:map/\${MapName}	aws:ResourceTag/\${TagKey} (p. 1218)
place-index	arn:\${Partition}:geo:\${Region}: \${Account}:place-index/\${IndexName}	aws:ResourceTag/\${TagKey} (p. 1218)
route-calculator	arn:\${Partition}:geo:\${Region}: \${Account}:route-calculator/ \${CalculatorName}	aws:ResourceTag/\${TagKey} (p. 1218)
tracker	arn:\${Partition}:geo:\${Region}: \${Account}:tracker/\${TrackerName}	aws:ResourceTag/\${TagKey} (p. 1218)

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 [Available global condition 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 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 \(p. 1219\)](#)
- [Resource types defined by Amazon Lookout for Equipment \(p. 1221\)](#)
- [Condition keys for Amazon Lookout for Equipment \(p. 1222\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1221)		
				aws:RequestTag/\${TagKey} (p. 1222)	
				aws:TagKeys (p. 1222)	
CreateInferenceScheduler	Grants permission to create an <code>InferenceScheduler</code> for a trained model	Write	inference-scheduler* (p. 1222)		
			model* (p. 1222)		
				aws:RequestTag/\${TagKey} (p. 1222)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys (p. 1222)	
CreateModel	Grants permission to create a model that is trained on a dataset	Write	dataset* (p. 1221)		
			model* (p. 1222)		
			aws:RequestTag/\${TagKey} (p. 1222)		aws:TagKeys (p. 1222)
DeleteDataset	Grants permission to delete a dataset	Write	dataset* (p. 1221)		
DeleteInferenceScheduler	Grants permission to delete an inference scheduler	Write	inference-scheduler* (p. 1222)		
DeleteModel	Grants permission to delete a model	Write	model* (p. 1222)		
DescribeDataIngestionJob	Grants permission to describe a data ingestion job	Read			
DescribeDataset	Grants permission to describe a dataset	Read	dataset* (p. 1221)		
DescribeInferenceScheduler	Grants permission to describe an inference scheduler	Read	inference-scheduler* (p. 1222)		
DescribeModel	Grants permission to describe a model	Read	model* (p. 1222)		
ListDataIngestionJobs	Grants permission to list the data ingestion jobs in your account or for a particular dataset	List	dataset* (p. 1221)		
ListDatasets	Grants permission to list the datasets in your account	List			
ListInferenceExecutions	Grants permission to list the inference executions for an inference scheduler	Read	inference-scheduler* (p. 1222)		
ListInferenceSchedulers	Grants permission to list the inference schedulers in your account	List			
ListModels	Grants permission to list the models in your account	List			
ListSensorStatistics	Grants permission to list the sensor statistics for a particular dataset or an ingestion job	List	dataset* (p. 1221)		
ListTagsForResource	Grants permission to list the tags for a resource	Read	dataset (p. 1221)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			inference-scheduler (p. 1222)		
			model (p. 1222)		
StartDataIngestion	Grants permission to start a data ingestion job for a dataset	Write	dataset* (p. 1221)		
StartInferenceScheduler	Grants permission to start an inference scheduler	Write	inference-scheduler* (p. 1222)		
StopInferenceScheduler	Grants permission to stop an inference scheduler	Write	inference-scheduler* (p. 1222)		
TagResource	Grants permission to tag a resource	Tagging	dataset (p. 1221)		
inference-scheduler (p. 1222)					
model (p. 1222)					
aws:RequestTag/ {\$TagKey} (p. 1222)					
UntagResource	Grants permission to untag a resource	Tagging	dataset (p. 1221)		
inference-scheduler (p. 1222)					
model (p. 1222)					
aws:TagKeys (p. 1222)					
UpdateInferenceScheduler	Grants permission to update an inference scheduler	Write	inference-scheduler* (p. 1222)		

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 \(p. 1219\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
dataset	arn:\${Partition}:lookoutequipment:\${Region}: \${AccountId}:dataset/\${DatasetName}/ \${DatasetId}	aws:ResourceTag/ {\$TagKey} (p. 1222)

Resource types	ARN	Condition keys
model	arn:\${Partition}:lookoutequipment:\${Region}:\${Account}:model/\${ModelName}/\${ModelError}	aws:ResourceTag/\${TagKey} (p. 1222)
inference-scheduler	arn:\${Partition}:lookoutequipment:\${Region}:\${Account}:inference-scheduler/\${InferenceSchedulerName}/\${InferenceSchedulerId}	aws:ResourceTag/\${TagKey} (p. 1222)

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 [Available global condition 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 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 \(p. 1222\)](#)
- [Resource types defined by Amazon Lookout for Metrics \(p. 1225\)](#)
- [Condition keys for Amazon Lookout for Metrics \(p. 1226\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1225)		
BackTestAnomalyDetector	Grants permission to run a backtest with an anomaly detector	Write	AnomalyDetector* (p. 1225)		
CreateAlert	Grants permission to create an alert for an anomaly detector	Write	Alert* (p. 1225)		
			AnomalyDetector* (p. 1225)		
			aws:RequestTag/ {\$TagKey} (p. 1226)		
CreateAnomalyDetector	Grants permission to create an anomaly detector	Write	AnomalyDetector* (p. 1225)		
			aws:RequestTag/ {\$TagKey} (p. 1226)		
			aws:TagKeys (p. 1226)		
CreateMetricSet	Grants permission to create a dataset	Write	AnomalyDetector* (p. 1225)		
			MetricSet* (p. 1225)		
			aws:RequestTag/ {\$TagKey} (p. 1226)		
DeactivateAnomalyDetector	Grants permission to deactivate an anomaly detector	Write	AnomalyDetector* (p. 1225)		
			aws:TagKeys (p. 1226)		
DeleteAlert	Grants permission to delete an alert	Write	Alert* (p. 1225)		
DeleteAnomalyDetector	Grants permission to delete an anomaly detector	Write	AnomalyDetector* (p. 1225)		
DescribeAlert	Grants permission to get details about an alert	Read	Alert* (p. 1225)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeAnomalyDetector	Grants permission to get information about an anomaly detection job	Read	AnomalyDetector* (p. 1225)		
DescribeAnomalyGroup	Grants permission to get details about an anomaly detector	Read	AnomalyDetector* (p. 1225)		
DescribeMetricSet	Grants permission to get details about a dataset	Read	MetricSet* (p. 1225)		
DetectMetricSetConfig	Grants permission to detect metric set config from data source	Write	AnomalyDetector* (p. 1225)		
GetAnomalyGroup	Grants permission to get details about a group of affected metrics	Read	AnomalyDetector* (p. 1225)		
GetDataQualityMetrics	Grants permission to get data quality metrics for an anomaly detector	Read	AnomalyDetector* (p. 1225)		
GetFeedback	Grants permission to get feedback on affected metrics for an anomaly group	Read	AnomalyDetector* (p. 1225)		
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 (p. 1225)		
ListAnomalyDetectors	Grants permission to get a list of anomaly detectors	List			
ListAnomalyGroups	Grants permission to get a list of related measures in an anomaly group	List	AnomalyDetector* (p. 1225)		
ListAnomalyGroups	Grants permission to get a list of anomaly groups	List	AnomalyDetector* (p. 1225)		
ListAnomalyGroups	Grants permission to get a list of affected metrics for a measure in an anomaly group	List	AnomalyDetector* (p. 1225)		
ListMetricSets	Grants permission to get a list of datasets	List	AnomalyDetector (p. 1225)		
ListTagsForResource	Grants permission to get a list of tags for a detector, dataset, or alert	Read	Alert (p. 1225)		
			AnomalyDetector (p. 1225)		
			MetricSet (p. 1225)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutFeedback	Grants permission to add feedback for an affected metric in an anomaly group	Write	AnomalyDetector* (p. 1225)		
TagResource	Grants permission to add tags to a detector, dataset, or alert	Tagging	Alert (p. 1225)		
			AnomalyDetector (p. 1225)		
			MetricSet (p. 1225)		
			aws:TagKeys (p. 1226) aws:RequestTag/ \${TagKey} (p. 1226) aws:ResourceTag/ \${TagKey} (p. 1226)		
UntagResource	Grants permission to remove tags from a detector, dataset, or alert	Tagging	Alert (p. 1225)		
AnomalyDetector (p. 1225)					
MetricSet (p. 1225)					
aws:TagKeys (p. 1226)					
UpdateAnomalyDetector	Grants permission to update an anomaly detector	Write	AnomalyDetector* (p. 1225)		
UpdateMetricSet	Grants permission to update a dataset	Write	MetricSet* (p. 1225)		

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](#) (p. 1222) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1226)
MetricSet	arn:\${Partition}:lookoutmetrics:\${Region}: \${Account}:MetricSet/\${AnomalyDetectorName}/ \${MetricSetName}	aws:ResourceTag/ \${TagKey} (p. 1226)
Alert	arn:\${Partition}:lookoutmetrics:\${Region}: \${Account}:Alert:\${AlertName}	aws:ResourceTag/ \${TagKey} (p. 1226)

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 [Available global condition 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 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 \(p. 1226\)](#)
- [Resource types defined by Amazon Lookout for Vision \(p. 1228\)](#)
- [Condition keys for Amazon Lookout for Vision \(p. 1229\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1229)		
			aws:RequestTag/\${TagKey} (p. 1229)		
			aws:TagKeys (p. 1229)		
CreateProject	Grants permission to create a new project	Write	project* (p. 1229)		
DeleteDataset	Grants permission to delete a dataset	Write			
DeleteModel	Grants permission to delete a model and all associated assets	Write	model* (p. 1229)		
DeleteProject	Grants permission to permanently remove a project	Write	project* (p. 1229)		
DescribeDataset	Grants permission to show detailed information about dataset manifest	Read			
DescribeModel	Grants permission to show detailed information about a model	Read	model* (p. 1229)		
DescribeModelPackageJob	Grants permission to show detailed information about a model packaging job	Read			
DescribeProject	Grants permission to show detailed information about a project	Read	project* (p. 1229)		
DescribeTrialDetectionState [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* (p. 1229)		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 resource	Read	model (p. 1229)		
ListTrialDetectionJobs [permission only]	Grants permission to list all anomaly detection jobs	List			
StartModel	Grants permission to start anomaly detection model	Write	model* (p. 1229)		
StartModelPackagingJob	Grants permission to start a model packaging job	Write	model* (p. 1229)		
StartTrialDetectionJob [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* (p. 1229)		
TagResource	Grants permission to tag a resource with given key value pairs	Tagging	model (p. 1229)		
			aws:RequestTag/\${TagKey} (p. 1229)	aws:TagKeys (p. 1229)	
UntagResource	Grants permission to remove the tag with the given key from a resource	Tagging	model (p. 1229)		
				aws:TagKeys (p. 1229)	
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 \(p. 1226\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1229)
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 [Available global condition 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 \(p. 1229\)](#)
- [Resource types defined by Amazon Machine Learning \(p. 1232\)](#)
- [Condition keys for Amazon Machine Learning \(p. 1233\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 (p. 1232)		
			datasource (p. 1232)		
			evaluation (p. 1232)		
			mlmodel (p. 1232)		
CreateBatchPrediction	Generates predictions for a group of observations	Write	batchprediction* (p. 1232)		
			datasource* (p. 1232)		
			mlmodel* (p. 1232)		
CreateDataSourceFromRDS	Creates a DataSource object from an Amazon RDS	Write	datasource* (p. 1232)		
CreateDataSourceFromRedshift	Creates a DataSource from a database hosted on an Amazon Redshift cluster	Write	datasource* (p. 1232)		
CreateDataSourceFromS3	Creates a DataSource object from S3	Write	datasource* (p. 1232)		
CreateEvaluation	Creates a new Evaluation of an MLModel	Write	datasource* (p. 1232)		
			evaluation* (p. 1232)		
			mlmodel* (p. 1232)		
CreateMLModel	Creates a new MLModel	Write	datasource* (p. 1232)		
			mlmodel* (p. 1232)		
CreateRealtimeEndpoint	Creates a real-time endpoint for the MLModel	Write	mlmodel* (p. 1232)		
DeleteBatchPrediction	Assigns the DELETED status to a BatchPrediction, rendering it unusable	Write	batchprediction* (p. 1232)		
DeleteDataSource	Assigns the DELETED status to a DataSource, rendering it unusable	Write	datasource* (p. 1232)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteEvaluation	Assigns the DELETED status to an Evaluation, rendering it unusable	Write	evaluation* (p. 1232)		
DeleteMLModel	Assigns the DELETED status to an MLModel, rendering it unusable	Write	mlmodel* (p. 1232)		
DeleteRealtimeEndpoint	Deletes a real time endpoint of an MLModel	Write	mlmodel* (p. 1232)		
DeleteTags	Deletes the specified tags associated with an ML object. After this operation is complete, you can't recover deleted tags	Tagging	batchprediction (p. 1232) datasource (p. 1232) evaluation (p. 1232) mlmodel (p. 1232)		
DescribeBatchPredictions	Returns a list of BatchPrediction operations that match the search criteria in the request	List			
DescribeDataSource	Returns a list of DataSource that match the search criteria in the request				
DescribeEvaluation	Returns a list of Descriptions that match the search criteria in the request	List			
DescribeMLModel	Returns a list of MLModel that match the search criteria in the request				
DescribeTags	Describes one or more of the tags for your Amazon ML object	List	batchprediction (p. 1232) datasource (p. 1232) evaluation (p. 1232) mlmodel (p. 1232)		
GetBatchPrediction	Returns a BatchPrediction that includes detailed metadata, status, and data file information		batchprediction* (p. 1232)		
GetDataSource	Returns a DataSource that includes metadata and data file information, as well as the current status of the DataSource		datasource* (p. 1232)		
GetEvaluation	Returns an Evaluation that includes metadata as well as the current status of the Evaluation		datasource* (p. 1232)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetMLModel	Returns an MLModel that includes detailed metadata, and data source information as well as the current status of the MLModel	Read	mlmodel* (p. 1232)		
Predict	Generates a prediction for the observation using the specified ML Model	Write	mlmodel* (p. 1232)		
UpdateBatchPrediction	Updates the BatchPredictionName of a BatchPrediction	Write	batchprediction* (p. 1232)		
UpdateDataSource	Updates the DataSourceName of a DataSource	Write	datasource* (p. 1232)		
UpdateEvaluation	Updates the EvaluationName of an Evaluation	Write	evaluation* (p. 1232)		
UpdateMLModel	Updates the MLModelName and the ScoreThreshold of an MLModel	Write	mlmodel* (p. 1232)		

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](#) (p. 1229) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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}	
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 [Available keys for conditions](#).

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 \(p. 1233\)](#)
- [Resource types defined by Amazon Macie \(p. 1239\)](#)
- [Condition keys for Amazon Macie \(p. 1239\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetCustomDataIdentifiers	Grants permission to retrieve information about one or more custom data identifiers	Read	CustomDataIdentifier* (p. 1239)		
CreateClassificationJob	Grants permission to create and define the settings for a sensitive data discovery job	Write	ClassificationJob* (p. 1239)	aws:RequestTag/ {\$TagKey} (p. 1239) aws:TagKeys (p. 1239)	
CreateCustomDataIdentifier	Grants permission to create and define the settings for a custom data identifier	Write	CustomDataIdentifier* (p. 1239)	aws:RequestTag/ {\$TagKey} (p. 1239) aws:TagKeys (p. 1239)	
CreateFindingsFilter	Grants permission to create and define the settings for a findings filter	Write	FindingsFilter* (p. 1239)	aws:RequestTag/ {\$TagKey} (p. 1239) aws:TagKeys (p. 1239)	
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* (p. 1239)	aws:RequestTag/ {\$TagKey} (p. 1239) aws:TagKeys (p. 1239)	
CreateSampleFindings	Grants permission to create sample findings	Write			
DeclineInvitations	Grants permission to decline Amazon Macie membership invitations	Write			
DeleteCustomDataIdentifier	Grants permission to delete a custom data identifier	Write	CustomDataIdentifier* (p. 1239)		
DeleteFindingsFilter	Grants permission to delete a findings filter	Write	FindingsFilter* (p. 1239)		
DeleteInvitations	Grants permission to delete Amazon Macie membership invitations	Write			

Service Authorization Reference
Service Authorization Reference
Amazon Macie

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteMember	Grants permission to delete the association between an Amazon Macie administrator account and an account	Write	Member* (p. 1239)		
DescribeBuckets	Grants permission to retrieve statistical data and other information about S3 buckets that Amazon Macie monitors and analyzes	Read			
DescribeClassificationJobs	Grants permission to retrieve information about the status and settings for a sensitive data discovery job	Read	ClassificationJob* (p. 1239)		
DescribeOrganizationConfiguration	Grants permission to retrieve information about the Amazon Macie configuration settings for an AWS organization	Read			
DisableMacie	Grants permission to disable an Amazon Macie account, which also deletes Macie resources for the account	Write			
DisableOrganizationAccountAsTheDelegatedAdministrator	Grants permission to disable an account as the delegated Amazon Macie administrator account for an AWS organization	Write			
DisassociateFromMemberAccountWith	Grants an Amazon Macie member account with permission to disassociate from its Macie administrator account	Write			
DisassociateFromMacieMember	(Deprecated) Grants an Amazon Macie member account with permission to disassociate from its Macie administrator account	Write			
DisassociateMemberAdministrator	Grants an Amazon Macie administrator account with permission to disassociate from a Macie member account	Write	Member* (p. 1239)		
EnableMacie	Grants permission to enable and specify the configuration settings for a new Amazon Macie account	Write			
EnableOrganizationAccountAsTheDelegatedAdministrator	Grants permission to enable an account as the delegated Amazon Macie administrator account for an AWS organization	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAdministratorInformation	Grants permission to retrieve information about the Amazon Macie administrator account for an account	Read			
GetBucketStatistics	Grants permission to retrieve aggregated statistical data for all the S3 buckets that Amazon Macie monitors and analyzes	Read			
GetClassificationSettingsForExporting	Grants permission to retrieve the settings for exporting sensitive data discovery results	Read			
GetCustomDataIdentifierInformation	Grants permission to retrieve information about the settings for a custom data identifier	Read	CustomDataIdentifier* (p. 1239)		
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* (p. 1239)		
GetFindingsPublicConfiguration	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			
GetMacieSession	Grants permission to retrieve information about the status and configuration settings for an Amazon Macie account	Read			
GetMasterAccount	(Deprecated) 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* (p. 1239)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
ListClassificationJobs	Grants permission to retrieve a subset of information about the status and settings for one or more sensitive data discovery jobs	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			
ListOrganizationAdministrators	Grants permission to retrieve information about the delegated, Amazon Macie administrator account for an AWS organization	List			
ListTagsForResource	Grants permission to retrieve the tags for an Amazon Macie resource	Read			
PutClassificationConfigurations	Grants permission to create or update configurations for storing sensitive data discovery results	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutFindingsPublic	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		aws:RequestTag/\${TagKey} (p. 1239)	aws:TagKeys (p. 1239)
TestCustomDataIdentifier	Grants permission to test a custom data identifier	Write			
UntagResource	Grants permission to remove tags from an Amazon Macie resource	Tagging		aws:TagKeys (p. 1239)	
UpdateClassificationStatus	Grants permission to change the status of a sensitive data discovery job	Write	ClassificationJob* (p. 1239)		
			aws:RequestTag/\${TagKey} (p. 1239)		aws:TagKeys (p. 1239)
UpdateFindingsFilter	Grants permission to update the settings for a findings filter	Write	FindingsFilter* (p. 1239)		
			aws:RequestTag/\${TagKey} (p. 1239)		aws:TagKeys (p. 1239)
UpdateMacieSession	Grants permission to suspend or re-enable an Amazon Macie account, or update the configuration settings for a Macie account	Write			
UpdateMemberSession	Grants an Amazon Macie administrator account with permission to suspend or re-enable a Macie member account	Write			
UpdateOrganizationMacieConfiguration	Grants permission to update configuration settings for an AWS organization	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 \(p. 1233\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
ClassificationJob	<code>arn:\${Partition}:macie2:\${Region}: \${Account}:classification-job/\${ResourceId}</code>	aws:ResourceTag/\${TagKey} (p. 1239)
CustomDataIdentifier	<code>arn:\${Partition}:macie2:\${Region}: \${Account}:custom-data-identifier/ \${ResourceId}</code>	aws:ResourceTag/\${TagKey} (p. 1239)
FindingsFilter	<code>arn:\${Partition}:macie2:\${Region}: \${Account}:findings-filter/\${ResourceId}</code>	aws:ResourceTag/\${TagKey} (p. 1239)
Member	<code>arn:\${Partition}:macie2:\${Region}: \${Account}:member/\${ResourceId}</code>	aws:ResourceTag/\${TagKey} (p. 1239)

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 [Available global condition keys](#).

Condition keys	Description	Type
aws:RequestTag/\${TagKey}	Filters access based on the presence of tag key-value pairs in the request	String
aws:ResourceTag/\${TagKey}	Filters access based on tag key-value pairs that are associated with the resource	String
aws:TagKeys	Filters access based on the presence of tag keys in the request	String

Actions, resources, and condition keys for Amazon Macie Classic

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

References:

- Learn how to [configure this service](#).
- View a list of the [API 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 Classic \(p. 1240\)](#)
- [Resource types defined by Amazon Macie Classic \(p. 1241\)](#)
- [Condition keys for Amazon Macie Classic \(p. 1241\)](#)

Actions defined by Amazon Macie Classic

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

The **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateMember	Enables the user to associate a specified AWS account with Amazon Macie as a member account.	Write			
AssociateS3Resources	Enables the user to associate specified S3 resources with Amazon Macie for monitoring and data classification.	Write		aws:SourceArn (p. 1241)	
DisassociateMember	Enables the user to remove the specified member account from Amazon Macie.	Write			
DisassociateS3Resources	Enables the user to remove specified S3 resources from being monitored by Amazon Macie.	Write		aws:SourceArn (p. 1241)	
ListMemberAccounts	Enables the user to list all Amazon Macie member accounts for the current Macie master account.	List			
ListS3Resources	Enables the user to list all the S3 resources associated with Amazon Macie.	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateS3Resources	Enables the user to update the classification types for the specified S3 resources.	Write		aws:SourceArn (p. 1241)	

Resource types defined by Amazon Macie Classic

Amazon Macie Classic does not support specifying a resource ARN in the Resource element of an IAM policy statement. To allow access to Amazon Macie Classic, specify “Resource”: “*” in your policy.

Condition keys for Amazon Macie Classic

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

To view the global condition keys that are available to all services, see [Available global condition keys](#).

Condition keys	Description	Type
aws:SourceArn	Allow access to the specified actions only when the request operates on the specified aws resource	Arn

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 \(p. 1241\)](#)
- [Resource types defined by Amazon Managed Blockchain \(p. 1244\)](#)
- [Condition keys for Amazon Managed Blockchain \(p. 1245\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateMember	Grants permission to create a member of an Amazon Managed Blockchain network	Write	network* (p. 1245)	iam:CreateServiceLinkedRole	
			aws:TagKeys (p. 1245)		
			aws:RequestTag/\${TagKey} (p. 1245)		
CreateNetwork	Grants permission to create an Amazon Managed Blockchain network	Write		aws:TagKeys (p. 1245)	iam:CreateServiceLinkedRole
CreateNode	Grants permission to create a node within a member of an Amazon Managed Blockchain network	Write	member (p. 1245)	iam:CreateServiceLinkedRole	
			network (p. 1245)		
			aws:TagKeys (p. 1245)		
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	aws:RequestTag/\${TagKey} (p. 1245)		
			network* (p. 1245)		
			aws:TagKeys (p. 1245)		
DeleteMember	Grants permission to delete a member and all associated resources from an Amazon Managed Blockchain network	Write	member* (p. 1245)		
DeleteNode	Grants permission to delete a node from a member of an Amazon Managed Blockchain network	Write	node* (p. 1245)		
GetMember	Grants permission to return detailed information about a member of an Amazon Managed Blockchain network	Read	member* (p. 1245)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetNetwork	Grants permission to return detailed information about an Amazon Managed Blockchain network	Read	network* (p. 1245)		
GetNode	Grants permission to return detailed information about a node within a member of an Amazon Managed Blockchain network	Read	node* (p. 1245)		
GetProposal	Grants permission to return detailed information about a proposal of an Amazon Managed Blockchain network	Read	proposal* (p. 1245)		
ListInvitations	Grants permission to list the invitations extended to the active AWS account from any Managed Blockchain network	List			
ListMembers	Grants permission to list the members of an Amazon Managed Blockchain network and the properties of their memberships	List	network* (p. 1245)		
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 (p. 1245)		
			network (p. 1245)		
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* (p. 1245)		
ListProposals	Grants permission to list proposals for the given Amazon Managed Blockchain network	List	network* (p. 1245)		
ListTagsForResource	Grants permission to view tags associated with an Amazon Managed Blockchain resource	Read	invitation (p. 1245)		
			member (p. 1245)		
			network (p. 1245)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			node (p. 1245)		
			proposal (p. 1245)		
RejectInvitation	Grants permission to reject the invitation to join the blockchain network	Write	invitation* (p. 1245)		
TagResource	Grants permission to add tags to an Amazon Managed Blockchain resource	Tagging	invitation (p. 1245) member (p. 1245) network (p. 1245) node (p. 1245) proposal (p. 1245)	aws:TagKeys (p. 1245) aws:RequestTag/\${TagKey} (p. 1245)	
UntagResource	Grants permission to remove tags from an Amazon Managed Blockchain resource	Tagging	invitation (p. 1245) member (p. 1245) network (p. 1245) node (p. 1245) proposal (p. 1245)	aws:TagKeys (p. 1245)	
UpdateMember	Grants permission to update a member of an Amazon Managed Blockchain network	Write	member* (p. 1245)	iam:CreateServiceLinkedRole (p. 1245)	
UpdateNode	Grants permission to update a node from a member of an Amazon Managed Blockchain network	Write	node* (p. 1245)	iam:CreateServiceLinkedRole (p. 1245)	
VoteOnProposal	Grants permission to cast a vote for a proposal on behalf of the blockchain network member specified	Write	proposal* (p. 1245)		

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 \(p. 1241\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you

can include in a policy. These keys are displayed in the last column of the 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} (p. 1245)
member	arn:\${Partition}:managedblockchain:\${Region}:\${Account}:members/\${MemberId}	aws:ResourceTag/\${TagKey} (p. 1245)
node	arn:\${Partition}:managedblockchain:\${Region}:\${Account}:nodes/\${NodeId}	aws:ResourceTag/\${TagKey} (p. 1245)
proposal	arn:\${Partition}:managedblockchain:\${Region}::proposals/\${ProposalId}	aws:ResourceTag/\${TagKey} (p. 1245)
invitation	arn:\${Partition}:managedblockchain:\${Region}:\${Account}:invitations/\${InvitationId}	aws:ResourceTag/\${TagKey} (p. 1245)

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 [Available global condition 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 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 \(p. 1246\)](#)
- [Resource types defined by Amazon Managed Grafana \(p. 1247\)](#)
- [Condition keys for Amazon Managed Grafana \(p. 1247\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
<code>AssociateLicense</code>	Grants permission to upgrade a workspace with a license	Write	<code>workspace*</code> (p. 1247)		<code>aws-marketplace:ViewSubscriptions</code>
<code>CreateWorkspace</code>	Grants permission to create a workspace	Write		<code>aws:TagKeys</code> (p. 1247) <code>aws:RequestTag</code> / <code>CreateManagedApplication</code> <code>[\$TagKey]</code> (p. 1248) <code>sso:DescribeRegisteredRegions</code> <code>sso:GetSharedSsoConfigurations</code>	
<code>CreateWorkspaceKey</code>	Grants permission to create API keys for a workspace	Write	<code>workspace*</code> (p. 1247)		
<code>DeleteWorkspace</code>	Grants permission to delete a workspace	Write	<code>workspace*</code> (p. 1247)		<code>sso:DeleteManagedApplication</code>
<code>DeleteWorkspaceKey</code>	Grants permission to delete API keys from a workspace	Write	<code>workspace*</code> (p. 1247)		
<code>DescribeWorkspace</code>	Grants permission to describe a workspace	Read	<code>workspace*</code> (p. 1247)		
<code>DescribeWorkspaceAuthentication</code>	Grants permission to describe authentication providers on a workspace	Read	<code>workspace*</code> (p. 1247)		
<code>DisassociateLicense</code>	Grants permission to remove a license from a workspace	Write	<code>workspace*</code> (p. 1247)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPermissions	Grants permission to list the permissions on a workspace	List	workspace*	(p. 1247)	
ListTagsForResource	Grants permission to list tags associated with a workspace	Read	workspace (p. 1247)		
ListWorkspaces	Grants permission to list workspaces	Read			
TagResource	Grants permission to add tags to, or update tag values of, a workspace	Tagging	workspace	(p. 1247)	
				aws:TagKeys (p. 1248)	
				aws:RequestTag/ \${TagKey} (p. 1248)	
UntagResource	Grants permission to remove tags from a workspace	Tagging	workspace	(p. 1247)	
				aws:TagKeys (p. 1248)	
				aws:RequestTag/ \${TagKey} (p. 1248)	
UpdatePermissions	Grants permission to modify the permissions on a workspace	Permissions management	workspace*	(p. 1247)	
UpdateWorkspace	Grants permission to modify a workspace	Write	workspace*	(p. 1247)	
UpdateWorkspaceAuthentication	Grants permission to modify authentication providers on a workspace	Write	workspace*	(p. 1247)	

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 \(p. 1246\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1248)

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters access by actions based on the presence of tag key-value pairs in the request	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters access by actions based on tag key-value pairs attached to the resource	String
<code>aws:TagKeys</code>	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 \(p. 1248\)](#)
- [Resource types defined by Amazon Managed Service for Prometheus \(p. 1252\)](#)
- [Condition keys for Amazon Managed Service for Prometheus \(p. 1252\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 <code>Alerts</code>	Write	workspace* (p. 1252)		
				aws:ResourceTag/ {\$TagKey} (p. 1252)	
CreateAlertManagerAlertDefinitions	Grants permission to create an <code>AlertDefinition</code>	Write	workspace* (p. 1252)		
				aws:ResourceTag/ {\$TagKey} (p. 1252)	
CreateRuleGroups	Grants permission to create a <code>rulegroups</code> namespace	Write	rulegroupsnamespace* (p. 1252)		
				aws:RequestTag/ {\$TagKey} (p. 1252)	
				aws:TagKeys (p. 1253)	
CreateWorkspace	Grants permission to create a workspace	Write		aws:RequestTag/ {\$TagKey} (p. 1252)	
				aws:TagKeys (p. 1253)	
DeleteAlertManagerAlertDefinitions	Grants permission to delete an <code>AlertDefinition</code>	Write	workspace* (p. 1252)		
				aws:ResourceTag/ {\$TagKey} (p. 1252)	
DeleteAlertManagerSilence	Grants permission to delete a <code>Silence</code>	Write	workspace* (p. 1252)		
				aws:ResourceTag/ {\$TagKey} (p. 1252)	
DeleteRuleGroups	Grants permission to delete a <code>rulegroups</code> namespace	Write	rulegroupsnamespace* (p. 1252)		
				aws:ResourceTag/ {\$TagKey} (p. 1252)	
DeleteWorkspace	Grants permission to delete a workspace	Write	workspace* (p. 1252)		
				aws:ResourceTag/ {\$TagKey} (p. 1252)	
DescribeAlertManagerAlertDefinitions	Grants permission to describe an <code>AlertDefinition</code>	Read	workspace* (p. 1252)		
				aws:ResourceTag/ {\$TagKey} (p. 1252)	
DescribeRuleGroups	Grants permission to describe a <code>rulegroups</code> namespace	Read	rulegroupsnamespace* (p. 1252)		
				aws:ResourceTag/ {\$TagKey} (p. 1252)	
DescribeWorkspace	Grants permission to describe a workspace	Read	workspace* (p. 1252)		
				aws:ResourceTag/ {\$TagKey} (p. 1252)	

Service Authorization Reference
 Service Authorization Reference
 Amazon Managed Service for Prometheus

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAlertManagerSilence	Grants permission to get a Silence	Read	workspace* (p. 1252)		
				aws:ResourceTag/ \${TagKey} (p. 1252)	
GetAlertManagerStatus	Grants permission to get current Status of an alertmanager	Read	workspace* (p. 1252)		
				aws:ResourceTag/ \${TagKey} (p. 1252)	
GetLabels	Grants permission to retrieve AMP workspace labels	Read	workspace* (p. 1252)		
				aws:ResourceTag/ \${TagKey} (p. 1252)	
GetMetricMetadata	Grants permission to retrieve the metadata for AMP workspace metrics	Read	workspace* (p. 1252)		
				aws:ResourceTag/ \${TagKey} (p. 1252)	
GetSeries	Grants permission to retrieve AMP workspace time series data	Read	workspace* (p. 1252)		
				aws:ResourceTag/ \${TagKey} (p. 1252)	
ListAlertManagerAlertGroups	Grants permission to list groups	Read	workspace* (p. 1252)		
				aws:ResourceTag/ \${TagKey} (p. 1252)	
ListAlertManagerAlerts	Grants permission to list alerts	Read	workspace* (p. 1252)		
				aws:ResourceTag/ \${TagKey} (p. 1252)	
ListAlertManagerReceivers	Grants permission to list Receivers	Read	workspace* (p. 1252)		
				aws:ResourceTag/ \${TagKey} (p. 1252)	
ListAlertManagerSilences	Grants permission to list silences	Read	workspace* (p. 1252)		
				aws:ResourceTag/ \${TagKey} (p. 1252)	
ListAlerts	Grants permission to list active alerts	Read	workspace* (p. 1252)		
				aws:ResourceTag/ \${TagKey} (p. 1252)	
ListRuleGroupsNamespaces	Grants permission to list rule groups namespaces	List	workspace* (p. 1252)		
				aws:ResourceTag/ \${TagKey} (p. 1252)	
ListRules	Grants permission to list alerting and recording rules	Read	workspace* (p. 1252)		

Service Authorization Reference
 Service Authorization Reference
 Amazon Managed Service for Prometheus

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/ \${TagKey} (p. 1252)	
ListTagsForResource	Grants permission to list tags on an AMP resource	Read	rulegroupsnamespace (p. 1252) workspace (p. 1252)	aws:TagKeys (p. 1253) aws:RequestTag/ \${TagKey} (p. 1252)	
ListWorkspaces	Grants permission to list workspaces	List			
PutAlertManagerDefinition	Grants permission to update an Alert manager definition	Write	workspace* (p. 1252)	aws:ResourceTag/ \${TagKey} (p. 1252)	
PutAlertManagerSilence	Grants permission to create or update a silence	Write	workspace* (p. 1252)	aws:ResourceTag/ \${TagKey} (p. 1252)	
PutRuleGroupsNamespace	Grants permission to update a rulegroups namespace	Write	rulegroupsnamespace* (p. 1252)	aws:ResourceTag/ \${TagKey} (p. 1252)	
QueryMetrics	Grants permission to run a query on AMP workspace metrics	Read	workspace* (p. 1252)	aws:ResourceTag/ \${TagKey} (p. 1252)	
RemoteWrite	Grants permission to perform a remote write operation to initiate the streaming of metrics to AMP workspace	Write	workspace* (p. 1252)	aws:ResourceTag/ \${TagKey} (p. 1252)	
TagResource	Grants permission to tag an AMP resource	Tagging	rulegroupsnamespace (p. 1252) workspace (p. 1252)	aws:TagKeys (p. 1253) aws:RequestTag/ \${TagKey} (p. 1252)	
UntagResource	Grants permission to untag an AMP resource	Tagging	rulegroupsnamespace (p. 1252) workspace (p. 1252)	aws:TagKeys (p. 1253) aws:RequestTag/ \${TagKey} (p. 1252)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateWorkspaceAlias	Grants permission to modify the alias of existing AMP workspace	Write	workspace* (p. 1252)		
				aws:ResourceTag/ {\$TagKey} (p. 1252)	

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 \(p. 1248\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1252) aws:ResourceTag/ {\$TagKey} (p. 1252) aws:TagKeys (p. 1253)
rulegroupsnamespace	arn:\${Partition}:aps:\${Region}: \${Account}:rulegroupsnamespace/ \${WorkspaceId}/\${Namespace}	aws:RequestTag/ {\$TagKey} (p. 1252) aws:ResourceTag/ {\$TagKey} (p. 1252) aws:TagKeys (p. 1253)

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 [Available global condition 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 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 \(p. 1253\)](#)
- [Resource types defined by Amazon Managed Streaming for Apache Kafka \(p. 1256\)](#)
- [Condition keys for Amazon Managed Streaming for Apache Kafka \(p. 1257\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchAssociateScramSecrets	Grants permission to associate one or more Scram Secrets with an Amazon MSK cluster	Write			kms:CreateGrant kms:RetireGrant
BatchDisassociateScramSecrets	Grants permission to disassociate one or more Scram	Write			kms:RetireGrant

Service Authorization Reference
 Service Authorization Reference
 Amazon Managed Streaming for Apache Kafka

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Secrets from an Amazon MSK cluster				
CreateCluster	Grants permission to create an MSK cluster	Write		aws:RequestTagKeys \${TagKey} (p. 1257)	ec2:DescribeSubnets aws:TagKeys (p. 1257) ec2:DescribeVpcs iam:AttachRolePolicy iam>CreateServiceLinkedRole iam:PutRolePolicy kms>CreateGrant kms:DescribeKey
CreateClusterV2	Grants permission to create an MSK cluster	Write		aws:RequestTagKeys \${TagKey} (p. 1257)	ec2>CreateVpcEndpoint aws:TagKeys (p. 1257) ec2>DeleteVpcEndpoints ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttributes ec2:DescribeVpcEndpoints ec2:DescribeVpcs iam:AttachRolePolicy iam>CreateServiceLinkedRole iam:PutRolePolicy kms>CreateGrant kms:DescribeKey
CreateConfiguration	Grants permission to create an MSK configuration	Write			
DeleteCluster	Grants permission to delete an MSK cluster	Write			ec2>DeleteVpcEndpoints ec2:DescribeVpcAttributes ec2:DescribeVpcEndpoints
DeleteConfiguration	Grants permission to delete the specified MSK configuration	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeCluster	Grants permission to describe an MSK cluster	Read			
DescribeClusterOperation	Grants permission to describe the <code>cluster</code> operation that is specified by the given ARN	Read			
DescribeClusterV2	Grants permission to describe an MSK cluster	Read			
DescribeConfiguration	Grants permission to describe an MSK configuration	Read	configuration* (p. 1257)		
DescribeConfigurationRevision	Grants permission to describe an MSK configuration revision	Read	configuration* (p. 1257)		
GetBootstrapBrokers	Grants permission to get connection details for the brokers in an MSK cluster	Read			
GetCompatibleKafkaVersions	Grants permission to get a list of other Apache Kafka versions to which you can update an MSK cluster	List			
ListClusterOperations	Grants permission to return a list of all the operations that have been performed on the specified MSK cluster	List			
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			
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			
ListScramSecrets	Grants permission to list the Scram Secrets associated with an Amazon MSK cluster	List			
ListTagsForResource	Grants permission to list tags of an MSK resource	Read	cluster (p. 1257)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RebootBroker	Grants permission to reboot broker	Write			
TagResource	Grants permission to tag an MSK resource	Tagging	cluster (p. 1257)		
				aws:RequestTag/\${TagKey} (p. 1257)	aws:TagKeys (p. 1257)
UntagResource	Grants permission to remove tags from an MSK resource	Tagging	cluster (p. 1257)		
				aws:TagKeys (p. 1257)	
UpdateBrokerCount	Grants permission to update the number of brokers of the MSK cluster	Write			
UpdateBrokerStorage	Grants permission to update the storage size of the brokers of the MSK cluster	Write			
UpdateBrokerType	Grants permission to update the broker type of an Amazon MSK cluster	Write			
UpdateClusterConfiguration	Grants permission to update the configuration of the MSK cluster	Write			
UpdateClusterKafkaVersion	Grants permission to update the MSK cluster to the specified Apache Kafka version	Write			
UpdateConfiguration	Grants permission to create a new revision of the MSK configuration	Write			
UpdateConnectivity	Grants permission to update the connectivity settings for the MSK cluster	Write			ec2:DescribeRouteTables ec2:DescribeSubnets
UpdateMonitoring	Grants permission to update the monitoring settings for the MSK cluster	Write			
UpdateSecurity	Grants permission to update the security settings for the MSK cluster	Write			kms:RetireGrant

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 \(p. 1253\)](#) identifies the resource

types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1257)
configuration	arn:\${Partition}:kafka:\${Region}: \${Account}:configuration/ \${ConfigurationName}/\${Uuid}	
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 [Available global condition 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 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 \(p. 1258\)](#)
- [Resource types defined by Amazon Managed Streaming for Kafka Connect \(p. 1259\)](#)
- [Condition keys for Amazon Managed Streaming for Kafka Connect \(p. 1260\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 logs>CreateLogDelivery logs:DescribeLogGroups logs:DescribeResourceLogs

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					logs:GetLogDelivery logs>ListLogDeliveries logs:PutResourcePolicy s3:GetBucketPolicy s3:PutBucketPolicy
CreateCustomPlugin	Grants permission to create an MSK Connect custom plugin	Write			s3GetObject
CreateWorkerConfig	Grants permission to create an MSK Connect worker configuration	Write			
DeleteConnector	Grants permission to delete an MSK Connect connector	Write			logs>DeleteLogDelivery logs>ListLogDeliveries
DeleteCustomPlugin	Grants permission to delete an MSK Connect custom plugin	Write			
DescribeConnector	Grants permission to describe an MSK Connect connector	Read	connector* (p. 1260)		
DescribeCustomPlugin	Grants permission to describe an MSK Connect custom plugin	Read	custom plugin* (p. 1260)		
DescribeWorkerConfig	Grants permission to describe an MSK Connect worker configuration	Read	worker configuration* (p. 1260)		
ListConnectors	Grants permission to list all MSK Connect connectors in this account	Read			
ListCustomPlugin	Grants permission to list all MSK Connect custom plugins in this account	Read			
ListWorkerConfig	Grants permission to list all MSK Connect worker configurations in this account	Read			
UpdateConnector	Grants permission to update an MSK Connect connector	Write			

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 \(p. 1258\)](#) identifies the resource

types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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}	
custom plugin	arn:\${Partition}:kafkaconnect: \${Region}: \${Account}:custom-plugin/ \${CustomPluginName}/\${UUID}	
worker configuration	arn:\${Partition}:kafkaconnect:\${Region}: \${Account}:worker-configuration/ \${WorkerConfigurationName}/\${UUID}	

Condition keys for Amazon Managed Streaming for Kafka Connect

MSK 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 [Available keys for conditions](#).

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 \(p. 1260\)](#)
- [Resource types defined by Amazon Managed Workflows for Apache Airflow \(p. 1262\)](#)
- [Condition keys for Amazon Managed Workflows for Apache Airflow \(p. 1262\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1262)		
CreateEnvironment	Grants permission to create an Amazon MWAA environment	Write	environment* (p. 1262)		
			aws:ResourceTag/ {\$TagKey} (p. 1263)		
			aws:RequestTag/ {\$TagKey} (p. 1263)		
			aws:TagKeys (p. 1263)		
CreateWebLoginToken	Grants permission to create a short-lived token that allows a user to log into Apache Airflow web UI	Write	rbac-role* (p. 1262)		
DeleteEnvironment	Grants permission to delete an Amazon MWAA environment	Write	environment* (p. 1262)		
			aws:ResourceTag/ {\$TagKey} (p. 1263)		
GetEnvironment	Grants permission to view details about an Amazon MWAA environment	Read	environment* (p. 1262)		
			aws:ResourceTag/ {\$TagKey} (p. 1263)		
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 (p. 1262)		
			aws:ResourceTag/ {\$TagKey} (p. 1263)		
PublishMetrics	Grants permission to publish metrics for an Amazon MWAA environment	Write	environment* (p. 1262)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to tag an Amazon MWAA environment	Tagging	environment (p. 1262)		
				aws:TagKeys (p. 1263)	
				aws:RequestTag/\${TagKey} (p. 1263)	
UntagResource	Grants permission to untag an Amazon MWAA environment	Tagging	environment (p. 1262)		
				aws:TagKeys (p. 1263)	
				aws:ResourceTag/\${TagKey} (p. 1263)	
UpdateEnvironment	Grants permission to modify an Amazon MWAA environment	Write	environment* (p. 1262)		
				aws:ResourceTag/\${TagKey} (p. 1263)	

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 \(p. 1260\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
<code>environment</code>	<code>arn:\${Partition}:airflow:\${Region}: \${Account}:environment/\${EnvironmentName}</code>	
<code>rbac-role</code>	<code>arn:\${Partition}:airflow:\${Region}: \${Account}:role/\${EnvironmentName}/ \${RoleName}</code>	

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 [Available global condition 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 \(p. 1263\)](#)
- [Resource types defined by AWS Marketplace \(p. 1265\)](#)
- [Condition keys for AWS Marketplace \(p. 1265\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 users to approve incoming subscription request (for ApproveVending)	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	providers who provide products that require subscription verification)				
CancelAgreement	Grants permission to users to cancel pending subscription requests for products that require subscription verification	Write			
DescribeAgreement	Grants permission to users to describe the metadata about the agreement	Read			
GetAgreementApprovers	Grants permission to users to view the details of their incoming subscription requests (for providers who provide products that require subscription verification)	Read			
GetAgreementReviewers	Grants permission to users to view the details of their subscription requests for data products that require subscription verification	Read			
GetAgreementTerms	Grants permission to users to get a list of terms for an agreement	List			
ListAgreementApprovers	Grants permission to users to list the incoming subscription requests (for providers who provide products that require subscription verification)	List			
ListAgreementReviewers	Grants permission to users to list their subscription requests for products that require subscription verification	List			
RejectAgreementRequest	Grants permission to users to decline a pending subscription requests (for providers who provide products that require subscription verification)	Write			
SearchAgreements	Grants permission to users to search their agreements	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Subscribe	Grants permission to users to subscribe to 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			
Unsubscribe	Grants permission to users to remove subscriptions to AWS Marketplace products. Includes the ability to disable auto-renewal for an existing subscription	Write			
UpdateAgreement <small>to make changes</small>	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			
ViewSubscription	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 [Available global condition keys](#).

Condition keys	Description	Type
aws-marketplace:AgreementType	Filters access by the type of the agreement.	String
aws-marketplace:PartyType	Filters access by the party type of the agreement.	String
aws-marketplace:ProductID	Filters access to AWS Marketplace RedHat OpenShift products in the RedHat console, based on the ProductID	String

Condition keys	Description	Type
	of the product. Note: This condition key only applies to the RedHat console, and using it will not allow access to products in AWS Marketplace.	

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 \(p. 1266\)](#)
- [Resource types defined by AWS Marketplace Catalog \(p. 1267\)](#)
- [Condition keys for AWS Marketplace Catalog \(p. 1268\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1267)		
CompleteTask	Grants permission to complete an existing task and submit the content to the associated change	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeChangeSets	Grants permission to return the details of an existing change set	Read	ChangeSet* (p. 1267)		
DescribeEntity	Grants permission to return the details of an existing entity	Read	Entity* (p. 1267)		
DescribeTask	Grants permission to return the details of an existing task	Read			
ListChangeSets	Grants permission to list existing change sets	List			
ListEntities	Grants permission to list existing entities	List			
ListTasks	Grants permission to list existing tasks	List			
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* (p. 1267)		
				catalog:ChangeType (p. 1268)	
UpdateTask	Grants permission to update the contents of an existing task	Write			

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 \(p. 1266\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
Entity	<code>arn:\${Partition}:aws-marketplace:\${Region}: \${Account}:#\${Catalog}/#\${EntityType}/ \${ResourceId}</code>	
ChangeSet	<code>arn:\${Partition}:aws-marketplace: \${Region}:#\${Account}:#\${Catalog}/ChangeSet/ \${ResourceId}</code>	

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 [Available global condition keys](#).

Condition keys	Description	Type
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 \(p. 1268\)](#)
- [Resource types defined by AWS Marketplace Commerce Analytics Service \(p. 1269\)](#)
- [Condition keys for AWS Marketplace Commerce Analytics Service \(p. 1269\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 [Available keys for conditions](#).

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.

Topics

- [Actions defined by AWS Marketplace Entitlement Service \(p. 1269\)](#)
- [Resource types defined by AWS Marketplace Entitlement Service \(p. 1270\)](#)
- [Condition keys for AWS Marketplace Entitlement Service \(p. 1270\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("**") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetEntitlements	Retrieves 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 [Available keys for conditions](#).

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 \(p. 1270\)](#)
- [Resource types defined by AWS Marketplace Image Building Service \(p. 1271\)](#)
- [Condition keys for AWS Marketplace Image Building Service \(p. 1271\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in

a statement with that action. 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.

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 [Available keys for conditions](#).

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 \(p. 1272\)](#)
- [Resource types defined by AWS Marketplace Management Portal \(p. 1272\)](#)

- Condition keys for AWS Marketplace Management Portal (p. 1273)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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 [Available keys for conditions](#).

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 \(p. 1273\)](#)
- [Resource types defined by AWS Marketplace Metering Service \(p. 1274\)](#)
- [Condition keys for AWS Marketplace Metering Service \(p. 1274\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterUsage	Grants permission to verify that the customer running your paid software is subscribed to your product on AWS Marketplace, enabling you to guard against unauthorized use. Meters software use per ECS task, per hour, with usage prorated to the second	Write			
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 [Available keys for conditions](#).

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 \(p. 1274\)](#)
- [Resource types defined by AWS Marketplace Private Marketplace \(p. 1276\)](#)
- [Condition keys for AWS Marketplace Private Marketplace \(p. 1276\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateProducts [permission only]	Grants permission to add new Approved products to the products to the Private Marketplace. Also allows 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			
CreatePrivateMarketplaceRequest [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 AWS Organization, provided the user has permissions to do so, and the Organization's Service Control Policies allow it.	Write			
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			
DisassociateProducts [permission only]	Grants permission to remove Approved products from the products from the Private Marketplace. Also allows to decline a request for a product to be associated with the Private Marketplace. This action can be performed	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	by any account in an AWS Organization, provided the user has permissions to do so, and the Organization's Service Control Policies allow it.				
ListPrivateMarketplaceProducts [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 [Available keys for conditions](#).

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 \(p. 1277\)](#)
- [Resource types defined by AWS Marketplace Procurement Systems Integration \(p. 1277\)](#)
- [Condition keys for AWS Marketplace Procurement Systems Integration \(p. 1278\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeProcurementSystemIntegration [permission only]	Describes 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			
PutProcurementSystem [permission only]	Creates or updates 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.	Write			

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 [Available keys for conditions](#).

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 \(p. 1278\)](#)
- [Resource types defined by Amazon Mechanical Turk \(p. 1282\)](#)
- [Condition keys for Amazon Mechanical Turk \(p. 1282\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateQualificationWithWorker	The AssociateQualificationWithWorker operation gives a Worker a Qualification	Write			
CreateAdditionalAssignmentsFor HIT	The CreateAdditionalAssignmentsFor HIT operation increases the maximum number of assignments of an existing HIT	Write			
Create HIT	The Create HIT operation creates a new HIT (Human Intelligence Task)	Write			
Create HIT Type	The Create HIT Type operation creates a new HIT type	Write			
Create HIT With HIT Type	The Create HIT With HIT Type operation creates a new Human Intelligence Task (HIT) using an existing HITTypeID generated by the Create HIT Type operation	Write			
Create Qualification Type	The Create Qualification Type operation creates a new Qualification type, which is represented by a QualificationType data structure	Write			
Create Worker Block	The Create Worker Block operation allows you to prevent a Worker from working on your HITs	Write			
Delete HIT	The Delete HIT operation disposes of a HIT that is no longer needed	Write			
Delete Qualification Type	The Delete Qualification Type operation disposes a Qualification type and disposes any HIT types that are associated with the Qualification type	Write			
Delete Worker Block	The Delete Worker Block operation allows you to reinstate a blocked Worker to work on your HITs	Write			
Disassociate Qualification From Worker	The Disassociate Qualification From Worker operation revokes a previously granted Qualification from a user	Write			

Service Authorization Reference
Service Authorization Reference
Amazon Mechanical Turk

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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 QualificationType for a QualificationRequirement	List			
ListQualificationRequests	The ListQualificationRequests operation retrieves requests for Qualifications of a particular Qualification type	List			

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendTestEventNotification	The <code>SendTestEventNotification</code> operation causes Amazon Mechanical Turk to send a notification message as if a HIT event occurred, according to the provided notification specification	Write			
UpdateExpirationForHIT	The <code>UpdateExpirationForHIT</code> operation allows you extend the expiration time of a HIT beyond its current expiration or expire a HIT immediately	Write			
UpdateHITReviewStatus	The <code>UpdateHITReviewStatus</code> operation toggles the status of a HIT	Write			
UpdateHITTypeOfHIT	The <code>UpdateHITTypeOfHIT</code> operation allows you to change the HITType properties of a HIT	Write			
UpdateNotificationSettings	The <code>UpdateNotificationSettings</code> operation creates, updates, disables or re-enables notifications for a HIT type	Write			
UpdateQualificationType	The <code>UpdateQualificationType</code> 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 [Available keys for conditions](#).

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 \(p. 1283\)](#)
- [Resource types defined by Amazon MemoryDB \(p. 1289\)](#)
- [Condition keys for Amazon MemoryDB \(p. 1289\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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
BatchUpdateClusters	Grants permissions to apply service updates	Write	cluster* (p. 1289)		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs s3:GetObject
					aws:ResourceTag/ \${TagKey} (p. 1290)
CopySnapshot	Grants permissions to make a copy of an existing snapshot	Write	snapshot* (p. 1289)		memorydb:TagResource s3:DeleteObject

Service Authorization Reference
Service Authorization Reference
Amazon MemoryDB

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					s3:GetBucketAcl s3:PutObject
					aws:ResourceTag/ \${TagKey} (p. 1290) aws:RequestTag/ \${TagKey} (p. 1289) aws:TagKeys (p. 1290)
CreateAcl	Grants permissions to create a new access control list	Write	user* (p. 1289) aws:ResourceTag/ \${TagKey} (p. 1290) aws:RequestTag/ \${TagKey} (p. 1289) aws:TagKeys (p. 1290)		memorydb:TagResource
CreateCluster	Grants permissions to create a cluster	Write	acl* (p. 1289) parametergroup* (p. 1289) subnetgroup* (p. 1289) snapshot (p. 1289) aws:ResourceTag/ \${TagKey} (p. 1290) aws:RequestTag/ \${TagKey} (p. 1289) aws:TagKeys (p. 1290)		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs memorydb:TagResource s3:GetObject
CreateParameterGroup	Grants permissions to create a new parameter group	Write			aws:RequestTag/ \${TagKey} (p. 1289) aws:TagKeys (p. 1290)

Service Authorization Reference
Service Authorization Reference
Amazon MemoryDB

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* (p. 1289)		memorydb:TagResource s3:DeleteObject s3:GetBucketAcl s3:PutObject
				aws:ResourceTag/\${TagKey} (p. 1290) aws:RequestTag/\${TagKey} (p. 1289) aws:TagKeys (p. 1290)	
CreateSubnetGroup	Grants permissions to create a new subnet group	Write	aws:RequestTag/\${TagKey} (p. 1289) aws:TagKeys (p. 1290)	memorydb:TagResource	
CreateUser	Grants permissions to create a new user	Write	aws:RequestTag/\${TagKey} (p. 1289) aws:TagKeys (p. 1290)	memorydb:TagResource	
DeleteAcl	Grants permissions to delete an access control list	Write	acl* (p. 1289)		
	aws:ResourceTag/\${TagKey} (p. 1290)				
DeleteCluster	Grants permissions to delete a previously provisioned cluster	Write	cluster* (p. 1289)		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
snapshot (p. 1289)					
	aws:ResourceTag/\${TagKey} (p. 1290)				
DeleteParameterGroup	Grants permissions to delete a parameter group	Write	parametergroup* (p. 1289)		
				aws:ResourceTag/\${TagKey} (p. 1290)	
DeleteSnapshot	Grants permissions to delete a snapshot	Write	snapshot* (p. 1289)		
				aws:ResourceTag/\${TagKey} (p. 1290)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteSubnetGroup	Grants permissions to delete a subnet group	Write	subnetgroup* (p. 1289)		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterface ec2:DescribeSubnets ec2:DescribeVpcs
					aws:ResourceTag/\${TagKey} (p. 1290)
DeleteUser	Grants permissions to delete a user	Write	user* (p. 1289)		aws:ResourceTag/\${TagKey} (p. 1290)
DescribeAcls	Grants permissions to retrieve information about access control lists	Read	acl* (p. 1289)		aws:ResourceTag/\${TagKey} (p. 1290)
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* (p. 1289)		aws:ResourceTag/\${TagKey} (p. 1290)
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			
DescribeParameterGroups	Grants permissions to retrieve information about parameter groups	Read	parametergroup* (p. 1289)		aws:ResourceTag/\${TagKey} (p. 1290)
DescribeParameters	Grants permissions to retrieve detailed parameter list for a particular parameter group	Read	parametergroup* (p. 1289)		aws:ResourceTag/\${TagKey} (p. 1290)
DescribeServiceUpdates	Grants permissions to retrieve details of the service updates	Read			
DescribeSnapshotDetails	Grants permissions to retrieve information about cluster snapshots	Read	snapshot* (p. 1289)		aws:ResourceTag/\${TagKey} (p. 1290)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeSubnetGroups	Grants permissions to retrieve a list of subnet groups	Read	subnetgroup* (p. 1289)		
				aws:ResourceTag/\${TagKey} (p. 1290)	
DescribeUsers	Grants permissions to retrieve information about users	Read	user* (p. 1289)		
				aws:ResourceTag/\${TagKey} (p. 1290)	
FailoverShard	Grants permissions to test automatic failover on a specified shard in a cluster	Write	cluster* (p. 1289)		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/\${TagKey} (p. 1290)	
ListNodeTypeUpdates	Grants permissions to list available node type updates	Read	cluster* (p. 1289)		
				aws:ResourceTag/\${TagKey} (p. 1290)	
ListTags	Grants permissions to list cost allocation tags	Read	acl (p. 1289)		
			cluster (p. 1289)		
			parametergroup (p. 1289)		
			snapshot (p. 1289)		
			subnetgroup (p. 1289)		
			user (p. 1289)		
			aws:ResourceTag/\${TagKey} (p. 1290)		
ResetParameterGroup	Grants permissions to modify the parameters of a parameter group to the engine or system default value	Write	parametergroup* (p. 1289)		
				aws:ResourceTag/\${TagKey} (p. 1290)	
TagResource	Grants permissions to add up to 10 cost allocation tags to the named resource	Tagging	acl (p. 1289)		
			cluster (p. 1289)		
			parametergroup (p. 1289)		
			snapshot (p. 1289)		
			subnetgroup (p. 1289)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			user (p. 1289) aws:TagKeys (p. 1290) aws:RequestTag/\${TagKey} (p. 1289) aws:ResourceTag/\${TagKey} (p. 1290)		
UntagResource	Grants permissions to remove the tags identified by the TagKeys list from a resource	Tagging	acl (p. 1289) cluster (p. 1289) parametergroup (p. 1289) snapshot (p. 1289) subnetgroup (p. 1289) user (p. 1289) aws:TagKeys (p. 1290) aws:ResourceTag/\${TagKey} (p. 1290)		
UpdateAcl	Grants permissions to update an access control list	Write	acl* (p. 1289) user* (p. 1289) aws:ResourceTag/\${TagKey} (p. 1290)		
UpdateCluster	Grants permissions to update the settings for a cluster	Write	cluster* (p. 1289) acl (p. 1289) parametergroup (p. 1289) aws:ResourceTag/\${TagKey} (p. 1290)		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
UpdateParameterGroup	Grants permissions to update parameters in a parameter group	Write	parametergroup* (p. 1289) aws:ResourceTag/\${TagKey} (p. 1290)		
UpdateSubnetGroup	Grants permissions to update a subnet group	Write	subnetgroup* (p. 1289)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/ \${TagKey} (p. 1290)	
UpdateUser	Grants permissions to update a user	Write	user* (p. 1289)		
				aws:ResourceTag/ \${TagKey} (p. 1290)	

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 \(p. 1283\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
parametergroup	arn:\${Partition}:memorydb:\${Region}:\${Account}:parametergroup/\${ParameterGroupName}	aws:ResourceTag/ \${TagKey} (p. 1290)
subnetgroup	arn:\${Partition}:memorydb:\${Region}:\${Account}:subnetgroup/\${SubnetGroupName}	aws:ResourceTag/ \${TagKey} (p. 1290)
cluster	arn:\${Partition}:memorydb:\${Region}:\${Account}:cluster/\${ClusterName}	aws:ResourceTag/ \${TagKey} (p. 1290)
snapshot	arn:\${Partition}:memorydb:\${Region}:\${Account}:snapshot/\${SnapshotName}	aws:ResourceTag/ \${TagKey} (p. 1290)
user	arn:\${Partition}:memorydb:\${Region}:\${Account}:user/\${UserName}	aws:ResourceTag/ \${TagKey} (p. 1290)
acl	arn:\${Partition}:memorydb:\${Region}:\${Account}:acl/\${AclName}	aws:ResourceTag/ \${TagKey} (p. 1290)

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 [Available global condition keys](#).

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	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:

- View a list of the [API operations available for this service](#).

Topics

- [Actions defined by Amazon Message Delivery Service \(p. 1290\)](#)
- [Resource types defined by Amazon Message Delivery Service \(p. 1291\)](#)
- [Condition keys for Amazon Message Delivery Service \(p. 1291\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
FailMessage	Grants permission to fail a message, signifying the message could not be processed successfully, ensuring it cannot be replied to or delivered again	Write			
GetEndpoint	Grants permission to route traffic to the correct endpoint based on the given destination for the messages	Read			
GetMessages	Grants permission to deliver messages to clients/instances using long polling	Read			
SendReply	Grants permission to send replies from clients/instances to upstream service	Write			

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

EC2 Messages 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 [Available keys for conditions](#).

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 \(p. 1292\)](#)
- [Resource types defined by AWS Microservice Extractor for .NET \(p. 1292\)](#)
- [Condition keys for AWS Microservice Extractor for .NET \(p. 1292\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
<code>GetConfig</code> [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 [Available keys for conditions](#).

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 \(p. 1293\)](#)

- [Resource types defined by AWS Migration Hub \(p. 1294\)](#)
- [Condition keys for AWS Migration Hub \(p. 1294\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateCreatedArtifactWithMigrationTask	Associate a given AWS artifact to a Migration Task	Write	migrationTask* (p. 1294)		
AssociateDiscoveryResultWithMigrationTask	Associate a given ADS resource to a Migration Task	Write	migrationTask* (p. 1294)		
CreateHomeRegionControl	Create a Migration Hub Home Region Control	Write			
CreateProgressUpdateStream	Create a ProgressUpdateStream	Write	progressUpdateStream* (p. 1294)		
DeleteProgressUpdateStream	Delete a ProgressUpdateStream	Write	progressUpdateStream* (p. 1294)		
DescribeApplicationService	Get an Application Discovery Service Application's state	Read			
DescribeHomeRegionControls	List Home Region Controls	List			
DescribeMigrationTask	Describe a Migration Task	Read	migrationTask* (p. 1294)		
DisassociateCreatedArtifactFromMigrationTask	Disassociate a given AWS artifact from a Migration Task	Write	migrationTask* (p. 1294)		
DisassociateDiscoveryResultFromMigrationTask	Disassociate a given ADS resource from a Migration Task	Write	migrationTask* (p. 1294)		
GetHomeRegion	Get the Migration Hub Home Region	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportMigrationTask	Import a MigrationTask	Write	migrationTask* (p. 1294)		
ListApplicationStates	List Application statuses	List			
ListCreatedArtifacts	List associated created artifacts for a MigrationTask	List	migrationTask* (p. 1294)		
ListDiscoveredResources	List associated ADS resources from MigrationTask	List	migrationTask* (p. 1294)		
ListMigrationTasks	List MigrationTasks	List			
ListProgressUpdateStreams	List ProgressUpdateStreams	List			
NotifyApplicationService	Update an Application Discovery Service Application's state	Write			
NotifyMigrationTaskState	Notify latest MigrationTask state	Write	migrationTask* (p. 1294)		
PutResourceAttributes	Put ResourceAttributes	Write	migrationTask* (p. 1294)		

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 \(p. 1293\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
progressUpdateStream	<code>arn:\${Partition}:mgh:\${Region}: \${Account}:progressUpdateStream/\${Stream}</code>	
migrationTask	<code>arn:\${Partition}:mgh:\${Region}: \${Account}:progressUpdateStream/\${Stream}/ migrationTask/\${Task}</code>	

Condition keys for AWS Migration Hub

Migration 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 [Available keys for conditions](#).

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 \(p. 1295\)](#)
- [Resource types defined by AWS Migration Hub Orchestrator \(p. 1298\)](#)
- [Condition keys for AWS Migration Hub Orchestrator \(p. 1298\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 workflow based on the selected template	Write		aws:RequestTag/\${TagKey} (p. 1298) aws:TagKeys (p. 1298)	
CreateWorkflowStep	Grants permission to create a step under a workflow and a specific step group	Write	workflow* (p. 1298)		
CreateWorkflowStepCustom	Grants permission to create a custom step group for a given workflow	Write	workflow* (p. 1298)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteWorkflow	Grants permission to a workflow	Write	workflow* (p. 1298)		
DeleteWorkflowStep	Grants permission to delete a Step from a specific step group under a workflow	Write	workflow* (p. 1298)		
DeleteWorkflowStepGroup	Grants permission to delete a Step group associated with a workflow	Write	workflow* (p. 1298)		
GetMessage	Grants permission to the plugin to receive information from the service	Read			
GetTemplate	Grants permission to get retrieve metadata for a Template	Read			
GetTemplateStep	Grants permission to retrieve details of a step associated with a template and a step group	Read			
GetTemplateStepGroup	Grants permission to retrieve metadata of a step group under a template	Read			
GetWorkflow	Grants permission to retrieve metadata associated with a workflow	Read	workflow* (p. 1298)		
GetWorkflowStep	Grants permission to get details of step associated with a workflow and a step group	Read	workflow* (p. 1298)		
GetWorkflowStepGroup	Grants permission to get details of step group associated with a workflow	Read	workflow* (p. 1298)		
ListPlugins	Grants permission to get a list all registered Plugins	List			
ListTagsForResource	Grants permission to get a list of all the tags tied to a resource	Read	workflow* (p. 1298)		
ListTemplateStepGroups	Grants permission to lists step groups of a template	List			
ListTemplateSteps	Grants permission to get a list of steps in a step group	List			
ListTemplates	Grants permission to get a list of all Templates available to customer	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListWorkflowStepGroups	Grants permission to get list of step groups associated with a workflow	List	workflow* (p. 1298)		
ListWorkflowSteps	Grants permission to get a list of steps within step group associated with a workflow	List	workflow* (p. 1298)		
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* (p. 1298)		
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* (p. 1298)		
StopWorkflow	Grants permission to stop a workflow	Write	workflow* (p. 1298)		
TagResource	Grants permission to add tags to a resource	Tagging	workflow* (p. 1298)		
				aws:TagKeys (p. 1298)	
UntagResource	Grants permission to remove tags from a resource	Tagging	workflow* (p. 1298)		
				aws:TagKeys (p. 1298)	
UpdateWorkflow	Grants permission to update the metadata associated with the workflow	Write	workflow* (p. 1298)		
UpdateWorkflowStep	Grants permission to update metadata and status of a custom step within a workflow	Write	workflow* (p. 1298)		
UpdateWorkflowStepGroup	Grants permission to update step group metadata associated with a step group in a given workflow	Write	workflow* (p. 1298)		

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 \(p. 1295\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
<code>workflow</code>	<code>arn:\${Partition}:migrationhub-orchestrator:\${Region}:\${Account}:workflow/\${ResourceId}</code>	<code>aws:ResourceTag/\${TagKey}</code> (p. 1298)

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters access by the tags that are passed in the request	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters access by the tags associated with the resource	String
<code>aws:TagKeys</code>	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 \(p. 1299\)](#)
- [Resource types defined by AWS Migration Hub Refactor Spaces \(p. 1304\)](#)
- [Condition keys for AWS Migration Hub Refactor Spaces \(p. 1304\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 (p. 1305) refactor-spaces:CreatedByAccountId (p. 1305) aws:RequestTag/\${TagKey} (p. 1305) aws:TagKeys (p. 1305)	
CreateEnvironment	Grants permission to create an environment	Write		aws:RequestTag/\${TagKey} (p. 1305) aws:TagKeys (p. 1305)	
CreateRoute	Grants permission to create a route within an application	Write		refactor-spaces:ApplicationCreatedByAccount (p. 1305) refactor-spaces:ServiceCreatedByAccount (p. 1305) refactor-spaces:RouteCreatedByAccount (p. 1305) refactor-spaces:CreatedByAccountId (p. 1305) refactor-spaces:SourcePath (p. 1305) aws:RequestTag/\${TagKey} (p. 1305) aws:TagKeys (p. 1305)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateService	Grants permission to create a service within an application	Write		refactor-spaces:ApplicationCreatedByAccount (p. 1304)	
DeleteApplication	Grants permission to delete an application from an environment	Write	application* (p. 1304)		
				refactor-spaces:ApplicationCreatedByAccount (p. 1304)	refactor-spaces:CreatedByAccountId (p. 1305)
DeleteEnvironment	Grants permission to delete an environment	Write	environment* (p. 1304)		
				aws:ResourceTag/\${TagKey} (p. 1305)	
DeleteResourcePolicy	Grants permission to delete a resource policy	Write			
DeleteRoute	Grants permission to delete a route from an application	Write	route* (p. 1304)		
				refactor-spaces:ApplicationCreatedByAccount (p. 1304)	refactor-spaces:ServiceCreatedByAccount (p. 1304)
DeleteService	Grants permission to delete a service from an application	Write	service* (p. 1304)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					refactor-spaces:ApplicationCreatedByAccount (p. 1304) refactor-spaces:ServiceCreatedByAccount (p. 1304) refactor-spaces:CreatedByAccountIds (p. 1305) aws:ResourceTag/\${TagKey} (p. 1305)
GetApplication	Grants permission to get more information about an application	Read	application*	(p. 1304)	
				refactor-spaces:ApplicationCreatedByAccount (p. 1304) refactor-spaces:CreatedByAccountIds (p. 1305) aws:ResourceTag/\${TagKey} (p. 1305)	
GetEnvironment	Grants permission to get more information for an environment	Read	environment*	(p. 1304)	
				aws:ResourceTag/\${TagKey} (p. 1305)	
GetResourcePolicy	Grants permission to get the details about a resource policy	Read			
GetRoute	Grants permission to get more information about a route	Read	route*	(p. 1304)	
				refactor-spaces:ApplicationCreatedByAccount (p. 1304) refactor-spaces:ServiceCreatedByAccount (p. 1304) refactor-spaces:RouteCreatedByAccount (p. 1305) refactor-spaces:CreatedByAccountIds (p. 1305) refactor-spaces:SourcePath (p. 1305) aws:ResourceTag/\${TagKey} (p. 1305)	
GetService	Grants permission to get more information about a service	Read	service*	(p. 1304)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				refactor-spaces:ApplicationCreatedByAccount (p. 1304)	
				refactor-spaces:ServiceCreatedByAccount (p. 1304)	
				refactor-spaces:CreatedByAccountId (p. 1305)	
				aws:ResourceTag/\${TagKey} (p. 1305)	
ListApplications	Grants permission to list all the applications in an environment	Read	environment* (p. 1304)		
ListEnvironmentVPCs	Grants permission to list all the VPCs for the environment	Read	environment* (p. 1304)		
ListEnvironments	Grants permission to list all environments	Read			
ListRoutes	Grants permission to list all the routes in an application	Read	environment* (p. 1304)		
ListServices	Grants permission to list all the services in an environment	Read	environment* (p. 1304)		
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 (p. 1304)		
			environment (p. 1304)		
			route (p. 1304)		
			service (p. 1304)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				refactor-spaces:ApplicationCreatedByAccount (p. 1305) refactor-spaces:ServiceCreatedByAccount (p. 1305) refactor-spaces:RouteCreatedByAccount (p. 1305) refactor-spaces:CreatedByAccountIds (p. 1305) refactor-spaces:SourcePath (p. 1305) aws:TagKeys (p. 1305) aws:RequestTag/\${TagKey} (p. 1305) aws:ResourceTag/\${TagKey} (p. 1305)	
UntagResource	Grants permission to remove a tag from a resource	Tagging	application (p. 1304) environment (p. 1304) route (p. 1304) service (p. 1304)	refactor-spaces:ApplicationCreatedByAccount (p. 1305) refactor-spaces:ServiceCreatedByAccount (p. 1305) refactor-spaces:RouteCreatedByAccount (p. 1305) refactor-spaces:CreatedByAccountIds (p. 1305) refactor-spaces:SourcePath (p. 1305) aws:TagKeys (p. 1305) aws:RequestTag/\${TagKey} (p. 1305) aws:ResourceTag/\${TagKey} (p. 1305)	

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 \(p. 1299\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
environment	<code>arn:\${Partition}:refactor-spaces:\${Region}: \${Account}:environment/\${EnvironmentId}</code>	aws:ResourceTag/\${TagKey} (p. 1305)
application	<code>arn:\${Partition}:refactor-spaces:\${Region}: \${Account}:environment/\${EnvironmentId}/ application/\${ApplicationId}</code>	aws:ResourceTag/\${TagKey} (p. 1305) refactor-spaces:ApplicationCreatedByAccount (p. 1305) refactor-spaces:CreatedByAccountIds (p. 1305)
service	<code>arn:\${Partition}:refactor-spaces:\${Region}: \${Account}:environment/\${EnvironmentId}/ application/\${ApplicationId}/service/ \${ServiceId}</code>	aws:ResourceTag/\${TagKey} (p. 1305) refactor-spaces:ApplicationCreatedByAccount (p. 1305) refactor-spaces:CreatedByAccountIds (p. 1305) refactor-spaces:ServiceCreatedByAccount (p. 1305)
route	<code>arn:\${Partition}:refactor-spaces:\${Region}: \${Account}:environment/\${EnvironmentId}/ application/\${ApplicationId}/route/ \${RouteId}</code>	aws:ResourceTag/\${TagKey} (p. 1305) refactor-spaces:ApplicationCreatedByAccount (p. 1305) refactor-spaces:CreatedByAccountIds (p. 1305) refactor-spaces:RouteCreatedByAccount (p. 1305) refactor-spaces:ServiceCreatedByAccount (p. 1305) refactor-spaces:SourcePath (p. 1305)

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters access by the presence of tag key-value pairs in the request	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters access by tag key-value pairs attached to the resource	String
<code>aws:TagKeys</code>	Filters access by the presence of tag keys in the request	ArrayOfString
<code>refactor-spaces:ApplicationCreated</code>	Filters access by restricting the action to only those accounts that created the application within an environment	String
<code>refactor-spaces:CreatedByAccountIds</code>	Filters access by the accounts that created the resource	ArrayOfString
<code>refactor-spaces:RouteCreated</code>	Filters access by restricting the action to only those accounts that created the route within an application	String
<code>refactor-spaces:ServiceCreated</code>	Filters access by restricting the action to only those accounts that created the service within an application	String
<code>refactor-spaces:SourcePath</code>	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 \(p. 1305\)](#)
- [Resource types defined by AWS Migration Hub Strategy Recommendations \(p. 1308\)](#)
- [Condition keys for AWS Migration Hub Strategy Recommendations \(p. 1308\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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			
GetApplicationCooperation	Grants permission to get details of an application	Read			
GetApplicationCompliance	Grants permission to get a list of compliance 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			
GetMessage	Grants permission to the collector to receive information from the service	Read			
GetPortfolioPreference	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			
GetRecommendationDetail	Grants permission to retrieve detailed information about a recommendation report	Read			
GetServerDetails	Grants permission to get info about a specific server	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetServerStrategies	Grants permission to get recommended strategies and tools for a specific server	Read			
ListAntiPatterns	Grants permission to get a list of all anti patterns that collector should look for in a customer's environment	List			
ListApplicationCode	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			
ListImportFileTasks	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			
ListServers	Grants permission to get a list of all servers in a customer's environment	List			
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			
StartImportFileTask	Grants permission to start importing data from a file provided by customer	Write			
StartRecommendationGeneration	Grants permission to start generating a recommendation report	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopAssessment	Grants permission to stop an ongoing assessment	Write			
UpdateApplication	Grants permission to update details for an application	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 [Available keys for conditions](#).

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 \(p. 1308\)](#)
- [Resource types defined by Amazon Mobile Analytics \(p. 1309\)](#)
- [Condition keys for Amazon Mobile Analytics \(p. 1309\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the **Resource** element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetFinancialReports for an app	Grant access to financial metrics	Read			
GetReports	Grant access to standard metrics for an app	Read			
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 [Available keys for conditions](#).

Actions, resources, and condition keys for AWS Mobile Hub

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

References:

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

Topics

- [Actions defined by AWS Mobile Hub \(p. 1310\)](#)
- [Resource types defined by AWS Mobile Hub \(p. 1311\)](#)
- [Condition keys for AWS Mobile Hub \(p. 1311\)](#)

Actions defined by AWS Mobile 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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateProject	Create a project	Write			
CreateServiceRole	Enable AWS Mobile Hub in the account by creating the required service role	Write			
DeleteProject	Delete the specified project	Write	project* (p. 1311)		
DeleteProjectSnapshot	Delete a saved snapshot of project configuration	Write			
DeployToStage	Deploy changes to the specified stage	Write			
DescribeBundle	Describe the download bundle	Read			
ExportBundle	Export the download bundle	Read			
ExportProject	Export the project configuration	Read	project* (p. 1311)		
GenerateProjectParameters	Generate project parameters required for code generation	Read	project* (p. 1311)		
GetProject	Get project configuration and resources	Read	project* (p. 1311)		
GetProjectSnapshot	Fetch the previously exported project configuration snapshot	Read			
ImportProject	Create a new project from the previously exported project configuration	Write			
InstallBundle	Install a bundle in the project deployments S3 bucket	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAvailableConnectors	List the available SaaS (Software as a Service) connectors	List			
ListAvailableFeatures	List available features	List			
ListAvailableRegions	List available regions for projects	List			
ListBundles	List the available download bundles	List			
ListProjectSnapshots	List saved snapshots of project configuration	List			
ListProjects	List projects	List			
SynchronizeProject	Synchronize state of resources into project	Write	project* (p. 1311)		
UpdateProject	Update project	Write	project* (p. 1311)		
ValidateProject	Validate a mobile hub project.	Read			
VerifyServiceRole	Verify AWS Mobile Hub is enabled in the account	Read			

Resource types defined by AWS Mobile 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 \(p. 1310\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
project	<code>arn:\${Partition}:mobilehub:\${Region}: \${Account}:project/\${ProjectId}</code>	

Condition keys for AWS Mobile Hub

Mobile 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 [Available keys for conditions](#).

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 \(p. 1312\)](#)
- [Resource types defined by Amazon Monitron \(p. 1314\)](#)
- [Condition keys for Amazon Monitron \(p. 1314\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateProjectWithUser [permission only]	Grants permission to associate a user with the project as an administrator	Permissions management	project* (p. 1314)		sso-directory:DescribeUsers sso:AssociateProfile sso:GetManagedApplications sso:GetProfile sso>ListDirectoryAssociations sso>ListProfiles

Service Authorization Reference
Service Authorization Reference
Amazon Monitron

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateProject [permission only]	Grants permission to create a project	Write		aws:RequestTag/ \${TagKey} (p. 1314) kms:CreateGrant aws:TagKeys (p. 1314) sso>CreateManagedApplication sso>DeleteManagedApplication	
DeleteProject [permission only]	Grants permission to delete a project	Write	project* (p. 1314)		sso>DeleteManagedApplication
DisassociateProjectAdministrator [permission only]	Grants permission to disassociate an administrator from the project	Permissions management	project* (p. 1314)		sso-directory:DescribeUsers sso:DisassociateProfile sso:GetManagedApplication sso:GetProfile sso>ListDirectoryAssociations sso>ListProfiles
GetProject [permission only]	Grants permission to get information about a project	Read	project* (p. 1314)		
GetProjectAdministrator [permission only]	Grants permission to describe an administrator who is associated with the project	Read	project* (p. 1314)		sso-directory:DescribeUsers sso:GetManagedApplication
ListProjectAdministrators [permission only]	Grants permission to list all administrators associated with the project	Permissions management	project* (p. 1314)		sso-directory:DescribeUsers sso:GetManagedApplication
ListProjects [permission only]	Grants permission to list all projects	List			
ListTagsForResource [permission only]	Grants permission to list all tags for a resource	Read	project (p. 1314)		
				aws:TagKeys (p. 1314)	aws:RequestTag/ \${TagKey} (p. 1314)
TagResource [permission only]	Grants permission to tag a resource	Tagging	project (p. 1314)		
				aws:TagKeys (p. 1314)	aws:RequestTag/ \${TagKey} (p. 1314)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagResource [permission only]	Grants permission to untag a resource	Tagging	project (p. 1314)		
				aws:TagKeys (p. 1314)	
UpdateProject [permission only]	Grants permission to update a project	Write	project* (p. 1314)		
				aws:TagKeys (p. 1314)	
				aws:RequestTag/ \${TagKey} (p. 1314)	

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 \(p. 1312\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1314)

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 [Available global condition 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 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 \(p. 1315\)](#)
- [Resource types defined by Amazon MQ \(p. 1317\)](#)
- [Condition keys for Amazon MQ \(p. 1318\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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} (p. 1318) aws:TagKeys (p. 1318)	ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2>CreateVpcEndpoint ec2:DescribeInternetGateway ec2:DescribeNetworkInterface ec2:DescribeNetworkInterfaceStatus ec2:DescribeSecurityGroup

Service Authorization Reference
Service Authorization Reference
Amazon MQ

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DescribeSubnets ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyNetworkInterface 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} (p. 1318) aws:TagKeys (p. 1318)
CreateTags	Grants permission to create tags	Tagging	brokers (p. 1318) configurations (p. 1318)		
					aws:RequestTag/\${TagKey} (p. 1318) aws:TagKeys (p. 1318)
CreateUser	Grants permission to create an ActiveMQ user	Write	brokers* (p. 1318)		
DeleteBroker	Grants permission to delete a broker	Write	brokers* (p. 1318)		ec2:DeleteNetworkInterface ec2:DeleteNetworkInterface ec2:DeleteVpcEndpoints ec2:DetachNetworkInterface
DeleteTags	Grants permission to delete tags	Tagging	brokers (p. 1318) configurations (p. 1318)		
					aws:TagKeys (p. 1318)
DeleteUser	Grants permission to delete an ActiveMQ user	Write	brokers* (p. 1318)		
DescribeBroker	Grants permission to return information about the specified broker	Read	brokers* (p. 1318)		
DescribeBrokerEngines	Grants permission to return information about broker engines	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeBrokerInformation	Grants permission to return information about the broker instance options	Read			
DescribeConfiguration	Grants permission to return information about the specified configuration	Read	configurations* (p. 1318)		
DescribeConfiguredRevision	Grants permission to return the specified configuration revision for the specified configuration	Read	configurations* (p. 1318)		
DescribeUser	Grants permission to return information about an ActiveMQ user	Read	brokers* (p. 1318)		
ListBrokers	Grants permission to return a list of all brokers	List			
ListConfigurations	Grants permission to return a list of all existing revisions for the specified configuration	List	configurations* (p. 1318)		
ListConfigurations	Grants permission to return a list of all configurations	List			
ListTags	Grants permission to return a list of tags	List	brokers (p. 1318)		
			configurations (p. 1318)		
ListUsers	Grants permission to return a list of all ActiveMQ users	List	brokers* (p. 1318)		
RebootBroker	Grants permission to reboot a broker	Write	brokers* (p. 1318)		
UpdateBroker	Grants permission to add a pending configuration change to a broker	Write	brokers* (p. 1318)		
UpdateConfiguration	Grants permission to update the specified configuration	Write	configurations* (p. 1318)		
UpdateUser	Grants permission to update the information for an ActiveMQ user	Write	brokers* (p. 1318)		

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](#) (p. 1315) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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:\${BrokerId}	aws:ResourceTag/\${TagKey} (p. 1318)
configurations	arn:\${Partition}:mq:\${Region}: \${Account}:configuration:\${ConfigurationId}	aws:ResourceTag/\${TagKey} (p. 1318)

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 [Available global condition keys](#).

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

Actions, resources, and condition keys for Amazon Neptune

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

References:

- View a list of the [API 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 \(p. 1318\)](#)
- [Resource types defined by Amazon Neptune \(p. 1319\)](#)
- [Condition keys for Amazon Neptune \(p. 1319\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
connect	Connect to database	Write	database* (p. 1319)		

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 \(p. 1318\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} : \${RelativeId}/database	

Condition keys for Amazon Neptune

Neptune 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 [Available keys for conditions](#).

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 \(p. 1320\)](#)
- [Resource types defined by AWS Network Firewall \(p. 1323\)](#)

- Condition keys for AWS Network Firewall (p. 1323)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateFirewallPolicy	Grants permission to create an association between a firewall policy and a firewall	Write	Firewall* (p. 1323)		
			FirewallPolicy* (p. 1323)		
AssociateSubnets	Grants permission to associate VPC subnets to a firewall	Write	Firewall* (p. 1323)		
CreateFirewall	Grants permission to create an AWS Network Firewall firewall	Write	Firewall* (p. 1323)		iam:CreateServiceLinkedRole
			FirewallPolicy* (p. 1323)		
			aws:RequestTag/\${TagKey} (p. 1323)		
			aws:TagKeys (p. 1323)		
CreateFirewallPolicy	Grants permission to create an AWS Network Firewall firewall policy	Write	FirewallPolicy* (p. 1323)		
			StatefulRuleGroup (p. 1323)		
			StatelessRuleGroup (p. 1323)		
			aws:RequestTag/\${TagKey} (p. 1323)		
CreateRuleGroup	Grants permission to create an AWS Network Firewall rule group	Write	StatefulRuleGroup (p. 1323)		
			StatelessRuleGroup (p. 1323)		
			aws:RequestTag/\${TagKey} (p. 1323)		
			aws:TagKeys (p. 1323)		

Service Authorization Reference
Service Authorization Reference
AWS Network Firewall

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteFirewall	Grants permission to delete a firewall	Write	Firewall* (p. 1323)		
DeleteFirewallPolicy	Grants permission to delete a firewall policy	Write	FirewallPolicy* (p. 1323)		
DeleteResourcePolicy	Grants permission to delete a resource policy for a firewall policy or rule group	Write	FirewallPolicy (p. 1323)		
			StatefulRuleGroup (p. 1323)		
			StatelessRuleGroup (p. 1323)		
DeleteRuleGroup	Grants permission to delete a rule group	Write	StatefulRuleGroup* (p. 1323)		
DescribeFirewall	Grants permission to retrieve the data objects that define a firewall	Read	Firewall* (p. 1323)		
DescribeFirewallPolicy	Grants permission to retrieve the data objects that define a firewall policy	Read	FirewallPolicy* (p. 1323)		
			StatefulRuleGroup (p. 1323)		
			StatelessRuleGroup (p. 1323)		
DescribeLogging	Grants permission to describe the logging configuration of a firewall	Read	Firewall* (p. 1323)		
DescribeResourcePolicy	Grants permission to describe a resource policy for a firewall policy or rule group	Read	FirewallPolicy (p. 1323)		
			StatefulRuleGroup (p. 1323)		
			StatelessRuleGroup (p. 1323)		
DescribeRuleGroup	Grants permission to retrieve the data objects that define a rule group	Read	StatefulRuleGroup (p. 1323)		
			StatelessRuleGroup (p. 1323)		
DescribeRuleGroupHighLevel	Grants permission to retrieve the high-level information about a rule group	Read	StatefulRuleGroup (p. 1323)		
			StatelessRuleGroup (p. 1323)		
DisassociateSubnets	Grants permission to disassociate VPC subnets from a firewall	Write	Firewall* (p. 1323)		
ListFirewallPolicies	Grants permission to retrieve the metadata for firewall policies	List	FirewallPolicy* (p. 1323)		
ListFirewalls	Grants permission to retrieve the metadata for firewalls	List	Firewall* (p. 1323)		
ListRuleGroups	Grants permission to retrieve the metadata for rule groups	List			

Service Authorization Reference
Service Authorization Reference
AWS Network Firewall

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to retrieve the tags for a resource	List	Firewall* (p. 1323)		
	FirewallPolicy* (p. 1323)				
	StatefulRuleGroup (p. 1323)				
	StatelessRuleGroup (p. 1323)				
PutResourcePolicy	Grants permission to put a resource policy for a firewall policy or rule group	Write	FirewallPolicy (p. 1323)		
	StatefulRuleGroup (p. 1323)				
	StatelessRuleGroup (p. 1323)				
TagResource	Grants permission to attach tags to a resource	Tagging	Firewall (p. 1323)		
	FirewallPolicy (p. 1323)				
	StatefulRuleGroup (p. 1323)				
	StatelessRuleGroup (p. 1323)				
	aws:RequestTag/ \${TagKey} (p. 1323)				
	aws:TagKeys (p. 1323)				
UntagResource	Grants permission to remove tags from a resource	Tagging	Firewall (p. 1323)		
	FirewallPolicy (p. 1323)				
	StatefulRuleGroup (p. 1323)				
	StatelessRuleGroup (p. 1323)				
	aws:TagKeys (p. 1323)				
UpdateFirewallDeleteOverrideProtection	Grants permission to add or remove protection for a firewall	Write	Firewall* (p. 1323)		
UpdateFirewallDescription	Grants permission to modify the description for a firewall	Write	Firewall* (p. 1323)		
UpdateFirewallPolicy	Grants permission to modify a firewall policy	Write	FirewallPolicy* (p. 1323)		
	StatefulRuleGroup (p. 1323)				
	StatelessRuleGroup (p. 1323)				
UpdateFirewallPolicyChangeProtection	Grants permission to add or remove firewall policy change protection for a firewall	Write	Firewall* (p. 1323)		
UpdateLoggingConfiguration	Grants permission to modify the logging configuration of a firewall	Write	Firewall* (p. 1323)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateRuleGroup	Grants permission to modify a rule group	Write	StatefulRuleGroup (p. 1323)		
			StatelessRuleGroup (p. 1323)		
UpdateSubnetChangeProtection	Grants permission to add subnet protection for a firewall	Write	Firewall* (p. 1323)		

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 \(p. 1320\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1323)
FirewallPolicy	arn:\${Partition}:network-firewall:\${Region}: \${Account}:firewall-policy/\${Name}	aws:ResourceTag/\${TagKey} (p. 1323)
StatefulRuleGroup	arn:\${Partition}:network-firewall:\${Region}: \${Account}:stateful-rulegroup/\${Name}	aws:ResourceTag/\${TagKey} (p. 1323)
StatelessRuleGroup	arn:\${Partition}:network-firewall:\${Region}: \${Account}:stateless-rulegroup/\${Name}	aws:ResourceTag/\${TagKey} (p. 1323)

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 [Available global condition 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 Manager

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 Network Manager \(p. 1324\)](#)
- [Resource types defined by Network Manager \(p. 1332\)](#)
- [Condition keys for Network Manager \(p. 1333\)](#)

Actions defined by 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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1332)		
AssociateConnectPeer	Grants permission to associate a <code>Connect Peer</code>	Write	device* (p. 1332)		
			global-network* (p. 1332)		
AssociateCustomerGateway	Grants permission to associate a <code>customer gateway</code> to a device	Write	device* (p. 1332)		
			global-network* (p. 1332)		

Service Authorization Reference
Service Authorization Reference
Network Manager

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			link (p. 1332)		
AssociateLink	Grants permission to associate a link to a device	Write	device* (p. 1332)		
			global-network* (p. 1332)		
			link* (p. 1332)		
AssociateTransitGatewayConnectPeer	Grants permission to associate a Transit Gateway Connect peer to a device	Write	device* (p. 1332)		
			global-network* (p. 1332)		
			link (p. 1332)		
				networkmanager:tgwConnectPeerArn	
CreateConnectAttachment	Grants permission to create a Connect attachment	Write	attachment* (p. 1332)		
			core-network* (p. 1332)		
				aws:RequestTag/\${TagKey} (p. 1333)	
CreateConnectPeer	Grants permission to create a Connect Peer connection	Write	attachment* (p. 1332)		
				aws:RequestTag/\${TagKey} (p. 1333)	
				aws:TagKeys (p. 1333)	
CreateConnection	Grants permission to create a new connection	Write	global-network* (p. 1332)		
				aws:RequestTag/\${TagKey} (p. 1333)	
				aws:TagKeys (p. 1333)	
CreateCoreNetwork	Grants permission to create a new core network	Write	global-network* (p. 1332)		
				aws:RequestTag/\${TagKey} (p. 1333)	
				aws:TagKeys (p. 1333)	
CreateDevice	Grants permission to create a new device	Write	global-network* (p. 1332)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 1333) aws:TagKeys (p. 1333)	
CreateGlobalNetwork	Grants permission to create a new global network	Write		aws:RequestTag/ \${TagKey} (p. 1333) aws:TagKeys (p. 1333)	ServiceLinkedRoleName (p. 1333)
CreateLink	Grants permission to create a new link	Write	global-network* (p. 1332) site (p. 1332)		
CreateSite	Grants permission to create a new site	Write	global-network* (p. 1332)		
CreateSiteToSiteVpnAttachment	Grants permission to create a Site-to-Site VPN attachment	Write	core-network* (p. 1332)		
CreateVpcAttachment	Grants permission to create a VPC attachment	Write	core-network* (p. 1332)		
DeleteAttachment	Grants permission to delete an attachment	Write	attachment* (p. 1332)		
DeleteConnectPeer	Grants permission to delete a Connect Peer	Write	connect-peer* (p. 1332)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteConnection	Grants permission to delete a connection	Write	connection* (p. 1332)		
			global-network* (p. 1332)		
DeleteCoreNetwork	Grants permission to delete a core network	Write	core-network* (p. 1332)		
DeleteCoreNetworkPolicyVersion	Grants permission to delete the core network policy version	Write	core-network* (p. 1332)		
DeleteDevice	Grants permission to delete a device	Write	device* (p. 1332)		
			global-network* (p. 1332)		
DeleteGlobalNetwork	Grants permission to delete a global network	Write	global-network* (p. 1332)		
DeleteLink	Grants permission to delete a link	Write	global-network* (p. 1332)		
			link* (p. 1332)		
DeleteResourceProvider	Grants permission to delete a resource provider	Write	core-network* (p. 1332)		
DeleteSite	Grants permission to delete a site	Write	global-network* (p. 1332)		
			site* (p. 1332)		
DeregisterTransitGateway	Grants permission to deregister a transit gateway from a global network	Write	global-network* (p. 1332)		
				networkmanager:tgwArn	(p. 1333)
DescribeGlobalNetworks	Grants permission to describe global networks	List	global-network (p. 1332)		
DisassociateConnectPeer	Grants permission to disassociate a Connect Peer	Write	global-network* (p. 1332)		
DisassociateCustomerGateway	Grants permission to disassociate a customer gateway from a device	Write	global-network* (p. 1332)		
				networkmanager:cgwArn	(p. 1333)
DisassociateLink	Grants permission to disassociate a link from a device	Write	device* (p. 1332)		
			global-network* (p. 1332)		
			link* (p. 1332)		
DisassociateTransitGatewayConnectPeer	Grants permission to disassociate a transit gateway connect peer from a device	Write	global-network* (p. 1332)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					networkmanager:tgwConnectPeerArn
ExecuteCoreNetworkChangesToTheCoreNetwork	Grants permission to apply changes to the core network	Write	core-network* (p. 1332)		
GetConnectAttachment	Grants permission to retrieve a Connect attachment	Read	attachment* (p. 1332)		
GetConnectPeer	Grants permission to retrieve a Connect Peer	Read	connect-peer* (p. 1332)		
GetConnectPeerAssociations	Grants permission to describe Connect Peer associations	Read	global-network* (p. 1332)		
GetConnections	Grants permission to describe connections	List	global-network* (p. 1332)		
			connection (p. 1332)		
GetCoreNetwork	Grants permission to retrieve a core network	Read	core-network* (p. 1332)		
GetCoreNetworkChangeSets	Grants permission to retrieve a list of core network change sets	Read	core-network* (p. 1332)		
GetCoreNetworkPolicy	Grants permission to retrieve a core network policy	Read	core-network* (p. 1332)		
GetCustomerGatewayAssociations	Grants permission to describe customer gateway associations	List	global-network* (p. 1332)		
GetDevices	Grants permission to describe devices	List	global-network* (p. 1332)		
			device (p. 1332)		
GetLinkAssociations	Grants permission to describe link associations	List	global-network* (p. 1332)		
			device (p. 1332)		
			link (p. 1332)		
GetLinks	Grants permission to describe links	List	global-network* (p. 1332)		
			link (p. 1332)		
GetNetworkResources	Grants permission to return the number of resources for a global network grouped by type	Read	global-network* (p. 1332)		
GetNetworkResourceRelationships	Grants permission to retrieve related resources for a resource within the global network	Read	global-network* (p. 1332)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetNetworkResources	Grants permission to retrieve a global network resource	Read	global-network* (p. 1332)		
GetNetworkRoutes	Grants permission to retrieve routes for a route table within the global network	Read	global-network* (p. 1332)		
GetNetworkTelemetry	Grants permission to retrieve network telemetry objects for the global network	Read	global-network* (p. 1332)		
GetResourcePolicy	Grants permission to retrieve a resource policy	Read	core-network* (p. 1332)		
GetRouteAnalysis	Grants permission to retrieve a route analysis configuration and result	Read	global-network* (p. 1332)		
GetSiteToSiteVpnAttachments	Grants permission to retrieve a site-to-site VPN attachment	Read	attachment* (p. 1332)		
GetSites	Grants permission to describe global networks	List	global-network* (p. 1332)		
			site (p. 1332)		
GetTransitGatewayConnections	Grants permission to describe transit gateway connections and peer associations	List	global-network* (p. 1332)		
GetTransitGatewayRegistrations	Grants permission to describe transit gateway registrations	List	global-network* (p. 1332)		
GetVpcAttachments	Grants permission to retrieve a VPC attachment	Read	attachment* (p. 1332)		
ListAttachments	Grants permission to describe attachments	List	attachment* (p. 1332)		
ListConnectPeers	Grants permission to describe Connect Peers	List	connect-peer* (p. 1332)		
ListCoreNetworkPolicyVersions	Grants permission to list core network policy versions	List	core-network* (p. 1332)		
ListCoreNetworks	Grants permission to list core networks	List			
ListOrganizationServiceAccessStatus	Grants permission to list Organization Service access status	List			
ListTagsForResource	Grants permission to list tags for a Network Manager resource	Read	attachment (p. 1332)		
			connect-peer (p. 1332)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			connection (p. 1332)		
	core-network (p. 1332)				
	device (p. 1332)				
	global-network (p. 1332)				
	link (p. 1332)				
	site (p. 1332)				
	aws:ResourceTag/\${TagKey} (p. 1333)				
PutCoreNetworkPolicy	Grants permission to create a core network policy	Write	core-network* (p. 1332)		
PutResourcePolicy	Grants permission to create or update a resource policy	Write	core-network* (p. 1332)		
RegisterTransitGateway	Grants permission to register a transit gateway to a global network	Write	global-network* (p. 1332)		
					networkmanager:tgwArn (p. 1333)
RejectAttachment	Grants permission to reject attachment request	Write	attachment* (p. 1332)		
RestoreCoreNetworkPolicy	Grants permission to restore the Policy Network policy to a previous version	Write	core-network* (p. 1332)		
StartOrganizationServiceUpdate	Grants permission to start Organization service update	Write			
StartRouteAnalysis	Grants permission to start route analysis and stores analysis configuration	Write	global-network* (p. 1332)		
TagResource	Grants permission to tag a Network Manager resource	Tagging	attachment (p. 1332)		
connect-peer (p. 1332)					
connection (p. 1332)					
core-network (p. 1332)					
device (p. 1332)					
global-network (p. 1332)					

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			link (p. 1332) site (p. 1332)		
				aws:TagKeys (p. 1333) aws:RequestTag/\${TagKey} (p. 1333) aws:ResourceTag/\${TagKey} (p. 1333)	
UntagResource	Grants permission to untag a Network Manager resource	Tagging	attachment (p. 1332)		
			connect-peer (p. 1332)		
			connection (p. 1332)		
			core-network (p. 1332)		
			device (p. 1332)		
			global-network (p. 1332)		
			link (p. 1332)		
			site (p. 1332)		
			aws:TagKeys (p. 1333)		
UpdateConnection	Grants permission to update a connection	Write	connection* (p. 1332)		
			global-network* (p. 1332)		
UpdateCoreNetwork	Grants permission to update a core network	Write	core-network* (p. 1332)		
UpdateDevice	Grants permission to update a device	Write	device* (p. 1332)		
			global-network* (p. 1332)		
UpdateGlobalNetwork	Grants permission to update a global network	Write	global-network* (p. 1332)		
UpdateLink	Grants permission to update a link	Write	global-network* (p. 1332)		
			link* (p. 1332)		
UpdateNetworkResource	Grants permission to add or update metadata key/value pairs on network resource	Write	global-network* (p. 1332)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateSite	Grants permission to update a site	Write	global-network* (p. 1332)		
			site* (p. 1332)		
UpdateVpcAttachment	Grants permission to update a VPC attachment	Write	attachment* (p. 1332)		
				aws:RequestTag/\${TagKey} (p. 1333)	
				aws:TagKeys (p. 1333)	
				networkmanager:subnetArns (p. 1333)	

Resource types defined by 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 \(p. 1324\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1333)
site	arn:\${Partition}:networkmanager::\${Account}:site/\${GlobalNetworkId}/ \${ResourceId}	aws:ResourceTag/\${TagKey} (p. 1333)
link	arn:\${Partition}:networkmanager::\${Account}:link/\${GlobalNetworkId}/ \${ResourceId}	aws:ResourceTag/\${TagKey} (p. 1333)
device	arn:\${Partition}:networkmanager::\${Account}:device/\${GlobalNetworkId}/ \${ResourceId}	aws:ResourceTag/\${TagKey} (p. 1333)
connection	arn:\${Partition}:networkmanager::\${Account}:connection/\${GlobalNetworkId}/ \${ResourceId}	aws:ResourceTag/\${TagKey} (p. 1333)
core-network	arn:\${Partition}:networkmanager::\${Account}:core-network/\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 1333)
attachment	arn:\${Partition}:networkmanager::\${Account}:attachment/\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 1333)
connect-peer	arn:\${Partition}:networkmanager::\${Account}:connect-peer/\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 1333)

Condition keys for Network Manager

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 [Available global condition 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:cgw ok disassociated	Filters access by which customer gateways can be associated	String
networkmanager:subnet move removed	Filters access by which VPC subnets can be added or removed from a VPC attachment	ArrayOfString
networkmanager:tgw register registered	Filters access by which transit gateways can be registered or deregistered	String
networkmanager:tgw associate associated	Filters access by which transit gateway connect peers can be associated	String
networkmanager:vpc attach attachment	Filters access by which VPC can be used to a create/update	String
networkmanager:vpn Create/update attachment	Filters access by which Site-to-Site VPN can be used to a Create/update attachment	String

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 \(p. 1334\)](#)
- [Resource types defined by Amazon Nimble Studio \(p. 1339\)](#)
- [Condition keys for Amazon Nimble Studio \(p. 1341\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1340)		
CreateLaunchProfile	Grants permission to create a launch profile	Write	studio* (p. 1339)		ec2:CreateNetworkInterface ec2:DescribeNatGateways ec2:DescribeNetworkAcls ec2:DescribeRouteTables ec2:DescribeSubnets ec2:DescribeVpcEndpoints ec2:RunInstances
			aws:TagKeys (p. 1341) aws:RequestTag/\${TagKey} (p. 1341)		
CreateStreamingImage	Grants permission to create a streaming image	Write	studio* (p. 1339)		ec2:DescribeImages ec2:DescribeSnapshots ec2:ModifyInstanceAttribute ec2:ModifySnapshotAttribute ec2:RegisterImage
			aws:TagKeys (p. 1341) aws:RequestTag/\${TagKey} (p. 1341)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateStreamingSession	Grants permission to create a Streaming session	Write	launch-profile* (p. 1340)		ec2:CreateNetworkInterface ec2:CreateNetworkInterface nimble:GetLaunchProfile nimble:GetLaunchProfile nimble>ListEulaAcceptance
			aws:TagKeys (p. 1341) aws:RequestTag/\${TagKey} (p. 1341)		
CreateStreamingSessionStream	Grants permission to create a Streaming Session Stream	Write	streaming-session* (p. 1340)		
			nimble:requesterPrincipalId (p. 1341)		
CreateStudio	Grants permission to create a studio	Write	studio* (p. 1339)		iam:PassRole sso>CreateManagedApplication
			aws:TagKeys (p. 1341) aws:RequestTag/\${TagKey} (p. 1341)		
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* (p. 1339)		ds:AuthorizeApplication ds:DescribeDirectories ec2:DescribeSecurityGroups fsx:DescribeFileSystems
			aws:TagKeys (p. 1341) aws:RequestTag/\${TagKey} (p. 1341)		
DeleteLaunchProfile	Grants permission to delete a Launch profile	Write	launch-profile* (p. 1340)		
DeleteLaunchProfileMember	Grants permission to delete a Launch profile member	Write	launch-profile* (p. 1340)		
DeleteStreamingImage	Grants permission to delete a Streaming image	Write	streaming-image* (p. 1340)		ec2>DeleteSnapshot ec2:DeregisterImage ec2:ModifyInstanceState ec2:ModifySnapshotAttribute

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteStreamingSession	Grants permission to delete a streaming session	Write	streaming-session* (p. 1340)		ec2:DeleteNetworkInterface
				nimble:requesterPrincipalId (p. 1341)	
DeleteStudio	Grants permission to delete a studio	Write	studio* (p. 1339)		sso>DeleteManagedApplication
DeleteStudioComponent	Grants permission to delete a studio component	Write	studio-component* (p. 1340)		ds:UnauthorizeApplication
DeleteStudioMember	Grants permission to delete a studio member	Write	studio* (p. 1339)		
GetEula	Grants permission to get a EULA	Read	eula* (p. 1340)		
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* (p. 1340)		
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* (p. 1340)		
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* (p. 1340)		ds:DescribeDirectories ec2:DescribeSecurityGroups fsx:DescribeFileSystems
GetLaunchProfileMember	Grants permission to get a launch profile member	Read	launch-profile* (p. 1340)		
GetStreamingImage	Grants permission to get a streaming image	Read	streaming-image* (p. 1340)		
GetStreamingSession	Grants permission to get a streaming session	Read	streaming-session* (p. 1340)		
				nimble:requesterPrincipalId (p. 1341)	
GetStreamingSessionStream	Grants permission to get a streaming session stream	Read	streaming-session* (p. 1340)		
				nimble:requesterPrincipalId (p. 1341)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetStudio	Grants permission to get a studio	Read	studio* (p. 1339)		
GetStudioComponent	Grants permission to get a studio component	Read	studio-component* (p. 1340)		
GetStudioMember	Grants permission to get a studio member	Read	studio* (p. 1339)		
ListEulaAcceptances	Grants permission to list EULA acceptances	Read	eula-acceptance* (p. 1341)		
ListEulas	Grants permission to list EULAs	Read	eula* (p. 1340)		
ListLaunchProfileMembers	Grants permission to list launch profile members	Read	launch-profile* (p. 1340)		
ListLaunchProfiles	Grants permission to list launch profiles	Read	studio* (p. 1339)		
				nimble:principalId (p. 1341)	
				nimble:requesterPrincipalId (p. 1341)	
ListStreamingImages	Grants permission to list streaming images	Read	studio* (p. 1339)		
ListStreamingSessions	Grants permission to list streaming sessions	Read	studio* (p. 1339)		
				nimble:createdBy (p. 1341)	
				nimble:ownedBy (p. 1341)	
				nimble:requesterPrincipalId (p. 1341)	
ListStudioComponents	Grants permission to list studio components	Read	studio* (p. 1339)		
ListStudioMembers	Grants permission to list studio members	Read	studio* (p. 1339)		
ListStudios	Grants permission to list all studios	Read			
ListTagsForResource	Grants permission to list all tags on a Nimble Studio resource	Read	launch-profile (p. 1340)		
			streaming-image (p. 1340)		
			streaming-session (p. 1340)		
			studio (p. 1339)		
			studio-component (p. 1340)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutLaunchProfile	Grants permission to add/ Update launch profile members	Write	launch-profile* (p. 1340)		sso-directory:DescribeUsers
PutStudioLogEvent [permission only]	Grants permission to report metrics and logs for the Nimble Studio portal to monitor application health	Write	studio* (p. 1339)		
PutStudioMember	Grants permission to add/ Update studio members	Write	studio* (p. 1339)		sso-directory:DescribeUsers
StartStreamingSession	Grants permission to start a streaming session	Write	streaming-session* (p. 1340)		nimble:GetLaunchProfile
					nimble:requesterPrincipalId (p. 1341)
StartStudioSSO	Grants permission to repair the studio's AWS SSO configuration	Write	studio* (p. 1339)		sso>CreateManagedApplication
StopStreamingSession	Grants permission to stop a streaming session	Write	streaming-session* (p. 1340)		nimble:GetLaunchProfile
					nimble:requesterPrincipalId (p. 1341)
TagResource	Grants permission to add or overwrite one or more tags for the specified Nimble Studio resource	Tagging	launch-profile (p. 1340)		
			streaming-image (p. 1340)		
			streaming-session (p. 1340)		
			studio (p. 1339)		
			studio-component (p. 1340)		
				aws:RequestTag/ {\$TagKey} (p. 1341)	
				aws:TagKeys (p. 1341)	
			aws:ResourceTag/ {\$TagKey} (p. 1341)		
UntagResource	Grants permission to disassociate one or more tags from the specified Nimble Studio resource	Tagging	launch-profile (p. 1340)		
			streaming-image (p. 1340)		
			streaming-session (p. 1340)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			studio (p. 1339)		
			studio-component (p. 1340)		
			aws:TagKeys (p. 1341)		
UpdateLaunchProfile	Grants permission to update a launch profile	Write	launch-profile* (p. 1340)		ec2:DescribeNatGateways ec2:DescribeNetworkAcls ec2:DescribeRouteTables ec2:DescribeSubnets ec2:DescribeVpcEndpoints
UpdateLaunchProfileMember	Grants permission to update a launch profile member	Write	launch-profile* (p. 1340)		
UpdateStreamingImage	Grants permission to update a streaming image	Write	streaming-image* (p. 1340)		
UpdateStudio	Grants permission to update a studio	Write	studio* (p. 1339)		iam:PassRole
UpdateStudioComponent	Grants permission to update a studio component	Write	studio-component* (p. 1340)		ds:AuthorizeApplication ds:DescribeDirectories ec2:DescribeSecurityGroups fsx:DescribeFileSystems

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 \(p. 1334\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1341) aws:ResourceTag/\${TagKey} (p. 1341) aws:TagKeys (p. 1341) nimble:studiod (p. 1341)

Resource types	ARN	Condition keys
streaming-image	<code>arn:\${Partition}:nimble:\${Region}: \${Account}:streaming-image/ \${StreamingImageId}</code>	aws:RequestTag/\${TagKey} (p. 1341) aws:ResourceTag/\${TagKey} (p. 1341) aws:TagKeys (p. 1341) nimble:studiod (p. 1341)
studio-component	<code>arn:\${Partition}:nimble:\${Region}: \${Account}:studio-component/ \${StudioComponentId}</code>	aws:RequestTag/\${TagKey} (p. 1341) aws:ResourceTag/\${TagKey} (p. 1341) aws:TagKeys (p. 1341) nimble:studiod (p. 1341)
launch-profile	<code>arn:\${Partition}:nimble:\${Region}: \${Account}:launch-profile/\${LaunchProfileId}</code>	aws:RequestTag/\${TagKey} (p. 1341) aws:ResourceTag/\${TagKey} (p. 1341) aws:TagKeys (p. 1341) nimble:studiod (p. 1341)
streaming-session	<code>arn:\${Partition}:nimble:\${Region}: \${Account}:streaming-session/ \${StreamingSessionId}</code>	aws:RequestTag/\${TagKey} (p. 1341) aws:ResourceTag/\${TagKey} (p. 1341) aws:TagKeys (p. 1341) nimble:createdBy (p. 1341) nimble:ownedBy (p. 1341)
eula	<code>arn:\${Partition}:nimble:\${Region}: \${Account}:eula/\${EulaId}</code>	aws:RequestTag/\${TagKey} (p. 1341) aws:ResourceTag/\${TagKey} (p. 1341) aws:TagKeys (p. 1341)

Resource types	ARN	Condition keys
eula-acceptance	arn:\${Partition}:nimble:\${Region}: \${Account}:eula-acceptance/ \${EulaAcceptanceId}	aws:RequestTag/\${TagKey} (p. 1341) aws:ResourceTag/\${TagKey} (p. 1341) aws:TagKeys (p. 1341) nimble:studiod (p. 1341)

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 [Available global condition 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	String
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:studiod	Filters access by a specific studio	ARN

Actions, resources, and condition keys for Amazon OpenSearch Service (successor to Amazon Elasticsearch Service)

Amazon OpenSearch Service (successor to Amazon Elasticsearch 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 \(successor to Amazon Elasticsearch Service\) \(p. 1342\)](#)
- [Resource types defined by Amazon OpenSearch Service \(successor to Amazon Elasticsearch Service\) \(p. 1350\)](#)
- [Condition keys for Amazon OpenSearch Service \(successor to Amazon Elasticsearch Service\) \(p. 1351\)](#)

Actions defined by Amazon OpenSearch Service (successor to Amazon Elasticsearch 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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptInboundCodeCredsFromCrossBoundaryRequest	Grants permission to the <code>destination</code> domain owner to accept an inbound cross-cluster search connection request	Write			
AcceptInboundCrossBoundaryConnection	Grants permission to the <code>destination</code> domain owner to accept an inbound cross-cluster search connection request. This permission is deprecated. Use <code>AcceptInboundConnection</code> instead	Write			
AddTags	Grants permission to attach resource tags to an OpenSearch Service domain	Tagging	domain* (p. 1350)		
			aws:RequestTag/ {\$TagKey} (p. 1351)		
			aws:TagKeys (p. 1351)		

Service Authorization Reference
 Service Authorization Reference
 Amazon OpenSearch Service (successor
 to Amazon Elasticsearch Service)

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* (p. 1350)		
CancelElasticsearchServiceSoftwareUpdate	Grants permission to cancel a service software update of a domain. This permission is deprecated. Use CancelServiceSoftwareUpdate instead	Write	domain* (p. 1350)		
CancelServiceSoftwareUpdate	Grants permission to cancel a service software update of a domain	Write	domain* (p. 1350)		
CreateDomain	Grants permission to create an Amazon OpenSearch Service domain	Write	domain (p. 1350)		
				aws:RequestTag/\${TagKey} (p. 1351) aws:TagKeys (p. 1351)	
CreateElasticsearchOpenSearchDomain	Grants permission to create an OpenSearch Service domain. This permission is deprecated. Use CreateDomain instead	Write	domain (p. 1350)		
				aws:RequestTag/\${TagKey} (p. 1351) aws:TagKeys (p. 1351)	
CreateElasticsearchServiceLinkedRole	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			
CreateOutboundConnection	Grants permission to create a new cross-cluster search connection from a source domain to a destination domain	Write	domain* (p. 1350)		
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* (p. 1350)		
CreatePackage	Grants permission to add a package for use with OpenSearch Service domains	Write			

Service Authorization Reference
 Service Authorization Reference
 Amazon OpenSearch Service (successor
 to Amazon Elasticsearch Service)

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			
DeleteDomain	Grants permission to delete an Amazon OpenSearch Service domain and all of its data	Write	domain* (p. 1350)		
DeleteElasticsearchOpenSearch	Grants permission to delete an OpenSearch Service domain and all of its data. This permission is deprecated. Use DeleteDomain instead	Write	domain* (p. 1350)		
DeleteElasticsearchServiceLinkedRole	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			
DeleteOutboundConnection	Grants permission to the source domain owner to delete an existing outbound cross-cluster search connection	Write			
DeleteOutboundCrossClusterSearchConnection	Grants permission to the source cluster 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			

Service Authorization Reference
 Service Authorization Reference
 Amazon OpenSearch Service (successor
 to Amazon Elasticsearch Service)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDomain	Grants permission to view a description of the domain configuration for the specified OpenSearch Service domain, including the domain ID, service endpoint, and ARN	Read	domain* (p. 1350)		
DescribeDomainAutoTune	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* (p. 1350)		
DescribeDomainConfigStageProgress	Grants permission to view the progress of an OpenSearch Service domain	Read	domain* (p. 1350)		
DescribeDomainConfig	Grants permission to view a description of the configuration options and status of an OpenSearch Service domain	Read	domain* (p. 1350)		
DescribeDomains	Grants permission to view a description of the domain configuration for up to five specified OpenSearch Service domains	List	domain* (p. 1350)		
DescribeElasticsearchDomainDescription	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* (p. 1350)		
DescribeElasticsearchDomainViewDescription	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* (p. 1350)		
DescribeElasticsearchDomainsDescription	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* (p. 1350)		

Service Authorization Reference
 Service Authorization Reference
 Amazon OpenSearch Service (successor
 to Amazon Elasticsearch Service)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeElasticsearchDomainTypeLimits	Grants permission to view the Instance Type Limits , storage, and master node limits for a given OpenSearch version and instance type. This permission is deprecated. Use DescribeInstanceTypeLimits instead	List			
DescribeInboundCrossClusterConnections	Grants permission to list all the Inbound Cross-Cluster Search Connections for a destination domain	List			
DescribeInboundCrossClusterConnections	Grants permission to list all the Cross-Cluster Search Connections for a destination domain. This permission is deprecated. Use DescribeInboundConnections instead	List			
DescribeInstanceTypeLimits	Grants permission to view the Instance Type Limits , storage, and master node limits for a given engine version and instance type	List			
DescribeOutboundCrossClusterConnections	Grants permission to list all the Outbound Cross-Cluster Search Connections for a source domain	List			
DescribeOutboundCrossClusterConnections	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			
DescribeReservedInstancesOfferings	Grants permission to fetch Reserved Instances Offerings offerings for Amazon OpenSearch Service. This permission is deprecated. Use DescribeReservedInstanceOfferings instead	List			

Service Authorization Reference
 Service Authorization Reference
 Amazon OpenSearch Service (successor
 to Amazon Elasticsearch Service)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeReservedOpenSearchServiceInstances	Grants permission to fetch OpenSearch Service Reserved Instances that have already been purchased. This permission is deprecated. Use DescribeReservedInstances instead	List			
DescribeReservedReservedInstancesOfferings	Grants permission to fetch Reserved Instance offerings for OpenSearch Service	List			
DescribeReservedOpenSearchServiceInstances	Grants permission to fetch OpenSearch Service Reserved Instances that have already been purchased	List			
DissociatePackage	Grants permission to disassociate a package from the specified OpenSearch Service domain	Write	domain* (p. 1350)		
ESCrossClusterGet	Grants permission to send cross-cluster requests to a destination domain	Read	domain (p. 1350)		
ESHttpDelete	Grants permission to send HTTP DELETE requests to the OpenSearch APIs	Write	domain (p. 1350)		
ESHttpGet	Grants permission to send HTTP GET requests to the OpenSearch APIs	Read	domain (p. 1350)		
ESHttpHead	Grants permission to send HTTP HEAD requests to the OpenSearch APIs	Read	domain (p. 1350)		
ESHttpPatch	Grants permission to send HTTP PATCH requests to the OpenSearch APIs	Write	domain (p. 1350)		
ESHttpPost	Grants permission to send HTTP POST requests to the OpenSearch APIs	Write	domain (p. 1350)		
ESHttpPut	Grants permission to send HTTP PUT requests to the OpenSearch APIs	Write	domain (p. 1350)		

Service Authorization Reference
 Service Authorization Reference
 Amazon OpenSearch Service (successor
 to Amazon Elasticsearch Service)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCompatibleEngineVersions	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* (p. 1350)		
GetCompatibleVersions	Grants permission to fetch a list of compatible engine versions to which an OpenSearch Service domain can be upgraded	List	domain* (p. 1350)		
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* (p. 1350)		
GetUpgradeStatus	Grants permission to fetch the upgrade status of a given OpenSearch Service domain	Read	domain* (p. 1350)		
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			
ListElasticsearchInstanceTypes	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			
ListElasticsearchSupportedVersions	Grants permission to list all supported OpenSearch versions on Amazon OpenSearch Service. This permission is deprecated. Use ListVersions instead	List			
ListInstanceTypeDetails	Grants permission to list all instance types and available features for a given OpenSearch or Elasticsearch version	List			

Service Authorization Reference
 Service Authorization Reference
 Amazon OpenSearch Service (successor
 to Amazon Elasticsearch Service)

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* (p. 1350)		
ListTags	Grants permission to display all resource tags for an OpenSearch Service domain	Read	domain* (p. 1350)		
ListVersions	Grants permission to list all supported OpenSearch and Elasticsearch versions in Amazon OpenSearch Service	List			
PurchaseReservedInstancesOffering	Grants permission to purchase Reserved Instances. This permission is deprecated. Use PurchaseReservedInstanceOffering instead	Write			
PurchaseReservedOpenSearchInstances	Grants permission to purchase OpenSearch reserved instances	Write			
RejectInboundConnection	Grants permission to the destination domain owner to reject an inbound cross-cluster search connection request	Write			
RejectInboundCrossClusterSearchConnection	Grants permission to the destination domain owner to reject an inbound cross-cluster search connection request. This permission is deprecated. Use RejectInboundConnection instead	Write			
RemoveTags	Grants permission to remove resource tags from an OpenSearch Service domain	Tagging	domain* (p. 1350)		
				aws:TagKeys (p. 1351)	
StartElasticsearchServiceSoftwareUpdate	Grants permission to start a service software update of a domain. This permission is deprecated. Use StartServiceSoftwareUpdate instead	Write	domain* (p. 1350)		
StartServiceSoftwareUpdate	Grants permission to start a service software update of a domain	Write	domain* (p. 1350)		

Service Authorization Reference
 Service Authorization Reference
 Amazon OpenSearch Service (successor
 to Amazon Elasticsearch Service)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateDomainConfig	Grants permission to modify the configuration of an OpenSearch Service domain, such as the instance type or number of instances	Write	domain* (p. 1350)		
UpdateElasticsearchConfiguration	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* (p. 1350)		
UpdatePackage	Grants permission to update a package for use with OpenSearch Service domains	Write			
UpgradeDomain	Grants permission to initiate upgrade of an OpenSearch Service domain to a given version	Write	domain* (p. 1350)		
UpgradeElasticsearch	Grants permission to initiate upgrade of an OpenSearch Service domain to a specified version. This permission is deprecated. Use UpgradeDomain instead	Write	domain* (p. 1350)		

Resource types defined by Amazon OpenSearch Service (successor to Amazon Elasticsearch 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 \(p. 1342\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1351)
es_role	arn:\${Partition}:iam::\${Account}:role/aws-service-role/es.amazonaws.com/AWSServiceRoleForAmazonOpenSearchService	aws:ResourceTag/\${TagKey} (p. 1351)
opensearchservice	arn:\${Partition}:iam::\${Account}:role/aws-service-role/	aws:ResourceTag/\${TagKey} (p. 1351)

Resource types	ARN	Condition keys
	opensearchservice.amazonaws.com/ AWSRoleForAmazonOpenSearchService	

Condition keys for Amazon OpenSearch Service (successor to Amazon Elasticsearch Service)

Amazon OpenSearch Service (successor to Amazon Elasticsearch 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 [Available global condition 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	String

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 \(p. 1351\)](#)
- [Resource types defined by AWS OpsWorks \(p. 1357\)](#)
- [Condition keys for AWS OpsWorks \(p. 1357\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 (p. 1357)		
AssignVolume	Grants permission to assign one of the stack's registered Amazon EBS volumes to a specified instance	Write	stack (p. 1357)		
AssociateElasticIp	Grants permission to associate one of the stack's registered Elastic IP addresses with a specified instance	Write	stack (p. 1357)		
AttachElasticLoadBalancer	Grants permission to attach an Elastic Load Balancing load balancer to a specified layer	Write	stack (p. 1357)		
CloneStack	Grants permission to create a clone of a specified stack	Write	stack (p. 1357)		
CreateApp	Grants permission to create an app for a specified stack	Write	stack (p. 1357)		
CreateDeployment	Grants permission to run deployment or stack commands	Write	stack (p. 1357)		
CreateInstance	Grants permission to create an instance in a specified stack	Write	stack (p. 1357)		
CreateLayer	Grants permission to create a layer	Write	stack (p. 1357)		
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 (p. 1357)		
DeleteInstance	Grants permission to delete a specified instance, which terminates the associated Amazon EC2 instance	Write	stack (p. 1357)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteLayer	Grants permission to delete a specified layer	Write	stack (p. 1357)		
DeleteStack	Grants permission to delete a specified stack	Write	stack (p. 1357)		
DeleteUserProfile	Grants permission to delete a user profile	Write			
DeregisterEcsClusters	Grants permission to delete a user profile	Write	stack (p. 1357)		
DeregisterElasticIps	Grants permission to deregister a specified Elastic IP address	Write	stack (p. 1357)		
DeregisterInstances	Grants permission to deregister a registered Amazon EC2 or on-premises instance	Write	stack (p. 1357)		
DeregisterRdsDbInstances	Grants permission to deregister an Amazon RDS instance	Write	stack (p. 1357)		
DeregisterVolumes	Grants permission to deregister an Amazon EBS volume	Write	stack (p. 1357)		
DescribeAgentVersions	Grants permission to describe the available AWS OpsWorks agent versions	List	stack (p. 1357)		
DescribeApps	Grants permission to request a description of a specified set of apps	List	stack (p. 1357)		
DescribeCommands	Grants permission to describe the results of specified commands	List	stack (p. 1357)		
DescribeDeployments	Grants permission to request a description of a specified set of deployments	List	stack (p. 1357)		
DescribeEcsClusters	Grants permission to describe Amazon ECS clusters that are registered with a stack	List	stack (p. 1357)		
DescribeElasticIps	Grants permission to describe Elastic IP addresses	List	stack (p. 1357)		
DescribeElasticLoadBalancers	Grants permission to describe a stack's Elastic Load Balancing instances	List	stack (p. 1357)		
DescribeInstances	Grants permission to request a description of a set of instances	List	stack (p. 1357)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeLayers	Grants permission to request a description of one or more layers in a specified stack	List	stack (p. 1357)		
DescribeLoadBasedScalingConfigurations	Grants permission to describe load-based auto scaling configurations for specified layers	List	stack (p. 1357)		
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 (p. 1357)		
DescribeRaidArrays	Grants permission to describe an instance's RAID arrays	List	stack (p. 1357)		
DescribeRdsDbInstances	Grants permission to describe Amazon RDS instances	List	stack (p. 1357)		
DescribeServiceErrors	Grants permission to describe AWS OpsWorks service errors	List	stack (p. 1357)		
DescribeStackProvisioningParameters	Grants permission to request a description of a stack's provisioning parameters	List	stack (p. 1357)		
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 (p. 1357)		
DescribeStacks	Grants permission to request a description of one or more stacks	List	stack (p. 1357)		
DescribeTimeBasedScalingConfigurations	Grants permission to describe time-based auto scaling configurations for specified instances	List	stack (p. 1357)		
DescribeUserProfiles	Grants permission to describe specified users	List			
DescribeVolumes	Grants permission to describe an instance's Amazon EBS volumes	List	stack (p. 1357)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DetachElasticLoadBalancer	Grants permission to detach a specified Elastic Load Balancing instance from its layer	Write	stack (p. 1357)		
DisassociateElasticIp	Grants permission to disassociate an Elastic IP address from its instance	Write	stack (p. 1357)		
GetHostnameSuggestions	Grants permission to get a generated host name for the specified layer, based on the current host name theme	Read	stack (p. 1357)		
GrantAccess	Grants permission to grant RDP access to a Windows instance for a specified time period	Write	stack (p. 1357)		
ListTags	Grants permission to return a list of tags that are applied to the specified stack or layer	List	stack (p. 1357)		
RebootInstance	Grants permission to reboot a specified instance	Write	stack (p. 1357)		
RegisterEcsCluster	Grants permission to register a specified Amazon ECS cluster with a stack	Write	stack (p. 1357)		
RegisterElasticIp	Grants permission to register an Elastic IP address with a specified stack	Write	stack (p. 1357)		
RegisterInstance	Grants permission to register instances with a specified stack that were created outside of AWS OpsWorks	Write	stack (p. 1357)		
RegisterRdsDbInstance	Grants permission to register an Amazon RDS instance with a stack	Write	stack (p. 1357)		
RegisterVolume	Grants permission to register an Amazon EBS volume with a specified stack	Write	stack (p. 1357)		
SetLoadBasedAutoScaling	Grants permission to specify the load-based auto scaling configuration for a specified layer	Write	stack (p. 1357)		
SetPermission	Grants permission to specify a user's permissions	Permissions management	stack (p. 1357)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SetTimeBasedAutoScaling	Grants permission to specify the time-based auto scaling configuration for a specified instance	Write	stack (p. 1357)		
StartInstance	Grants permission to start a specified instance	Write	stack (p. 1357)		
StartStack	Grants permission to start a stack's instances	Write	stack (p. 1357)		
StopInstance	Grants permission to stop a specified instance	Write	stack (p. 1357)		
StopStack	Grants permission to stop a specified stack	Write	stack (p. 1357)		
TagResource	Grants permission to apply tags to a specified stack or layer	Tagging	stack (p. 1357)		
UnassignInstance	Grants permission to unassign a registered instance from all of it's layers	Write	stack (p. 1357)		
UnassignVolume	Grants permission to unassign an assigned Amazon EBS volume	Write	stack (p. 1357)		
UntagResource	Grants permission to remove tags from a specified stack or layer	Tagging	stack (p. 1357)		
UpdateApp	Grants permission to update a specified app	Write	stack (p. 1357)		
UpdateElasticIp	Grants permission to update a registered Elastic IP address's name	Write	stack (p. 1357)		
UpdateInstance	Grants permission to update a specified instance	Write	stack (p. 1357)		
UpdateLayer	Grants permission to update a specified layer	Write	stack (p. 1357)		
UpdateMyUserProfile	Grants permission to update a user's SSH public key	Write			
UpdateRdsDbInstance	Grants permission to update an Amazon RDS instance	Write	stack (p. 1357)		
UpdateStack	Grants permission to update a specified stack	Write	stack (p. 1357)		
UpdateUserProfile	Grants permission to update a specified user profile	Permissions management			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateVolume	Grants permission to update an Amazon EBS volume's name or mount point	Write	stack (p. 1357)		

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 \(p. 1351\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
stack	<code>arn:\${Partition}:opsworks:\${Region}: \${Account}:stack/\${StackId}/</code>	

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 [Available keys for conditions](#).

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 \(p. 1357\)](#)
- [Resource types defined by AWS OpsWorks Configuration Management \(p. 1359\)](#)
- [Condition keys for AWS OpsWorks Configuration Management \(p. 1360\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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			
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			
DescribeAccountAssociations	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			
DescribeNodeAssociations	Grants permission to describe the association status for the specified node token and the specified server	List			
DescribeServers	Grants permission to describe the specified server or all servers of the user's account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
UpdateServer	Grants permission to update general server settings	Write			
UpdateServerEngineSettings	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 \(p. 1357\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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 [Available keys for conditions](#).

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 \(p. 1360\)](#)
- [Resource types defined by AWS Organizations \(p. 1366\)](#)
- [Condition keys for AWS Organizations \(p. 1366\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1366)		
AttachPolicy	Grants permission to attach a policy to a root, an	Write	policy* (p. 1366)		

Service Authorization Reference
Service Authorization Reference
AWS Organizations

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	organizational unit, or an individual account		account (p. 1366)		
			organizationalunit (p. 1366)		
			root (p. 1366)		
				organizations:PolicyType (p. 1367)	
CancelHandshake	Grants permission to cancel a handshake	Write	handshake* (p. 1366)		
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* (p. 1366)		
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} (p. 1367) aws:TagKeys (p. 1367)		
CreateGovCloudAccount	Grants permission to create an AWS GovCloud (US) account	Write	aws:RequestTag/ \${TagKey} (p. 1367) aws:TagKeys (p. 1367)		
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			
CreateOrganizationalUnit	Grants permission to create an organizational unit (OU) within a root or parent OU	Write	organizationalunit (p. 1366)		
root (p. 1366)					
aws:RequestTag/ \${TagKey} (p. 1367)			aws:TagKeys (p. 1367)		
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 (p. 1367) aws:RequestTag/ \${TagKey} (p. 1367) aws:TagKeys (p. 1367)		

Service Authorization Reference
Service Authorization Reference
AWS Organizations

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeclineHandshake	Grants permission to decline a handshake request. This sets the handshake state to DECLINED and effectively deactivates the request	Write	handshake* (p. 1366)		
DeleteOrganization	Grants permission to delete the organization	Write			
DeleteOrganizationalUnit	Grants permission to delete an organizational unit from a root or another OU	Write	organizationalunit* (p. 1366)		
DeletePolicy	Grants permission to delete a policy from your organization	Write	policy* (p. 1366)		
DeregisterDelegatedAdministrator	Grants permission to deregister the specified member AWS account as a delegated administrator for the AWS service that is specified by ServicePrincipal		account* (p. 1366)		organizations:ServicePrincipal (p. 1367)
DescribeAccount	Grants permission to retrieve Organizations-related details about the specified account	Read	account* (p. 1366)		
DescribeCreateAccountRequest	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* (p. 1366)		
DescribeHandshake	Grants permission to retrieve details about a previously requested handshake		handshake* (p. 1366)		
DescribeOrganization	Grants permission to retrieves details about the organization that the calling credentials belong to	Read			
DescribeOrganizationalUnit	Grants permission to retrieves details about an organizational unit (OU)	Read	organizationalunit* (p. 1366)		
DescribePolicy	Grants permission to retrieves details about a policy	Read	policy* (p. 1366)		
					organizations:PolicyType (p. 1367)

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* (p. 1366) account (p. 1366) organizationalunit (p. 1366) root (p. 1366)		
			organizations:PolicyType (p. 1367)		
			organizations:ServicePrincipal (p. 1367)		
			organizations:PolicyType (p. 1367)		
DisableAWSServiceIntegration	Grants permission to disable integration of an AWS service (the service that is specified by ServicePrincipal) with AWS Organizations	Write	root* (p. 1366)		
			organizations:PolicyType (p. 1367)		
EnableAWSServiceIntegration	Grants permission to enable integration of an AWS service (the service that is specified by ServicePrincipal) with AWS Organizations	Write			organizations:ServicePrincipal (p. 1367)
EnableAllFeatures	Grants permission to start the process to enable all features in an organization, upgrading it from supporting only Consolidated Billing features	Write			
			organizations:PolicyType (p. 1367)		
InviteAccountToOrganization	Grants permission to send an invitation to another AWS account, asking it to join your organization as a member account	Write	account (p. 1366) aws:RequestTag/\${TagKey} (p. 1367) aws:TagKeys (p. 1367)		
LeaveOrganization	Grants permission to remove a member account from its parent organization	Write			
ListAWSServiceAccounts	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			

Service Authorization Reference
Service Authorization Reference
AWS Organizations

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAccountsForParent	Grants permission to list the accounts in an organization that are contained by a root or organizational unit (OU)	List	organizationalunit (p. 1366)		
			root (p. 1366)		
ListChildren	Grants permission to list all of the OUs or accounts that are contained in a parent OU or root	List	organizationalunit (p. 1366)		
			root (p. 1366)		
ListCreateAccountSync	Grants permission to list the synchronous account creation requests that are currently being tracked for the organization	List			
ListDelegatedAdmins	Grants permission to list the AWS accounts that are designated as delegated administrators in this organization	List			organizations:ServicePrincipal (p. 1367)
ListDelegatedServices	Grants permission to list the AWS services for which the specified account is a delegated administrator in this organization	List	account* (p. 1366)		
ListHandshakesForHandshake	Grants permission to list all the handshakes that are associated with an account	List			
ListHandshakesForOrganization	Grants permission to list the handshakes that are associated with the organization	List			
ListOrganizationalUnitsForParent	Grants permission to lists all of the organizational units (OUs) in a parent organizational unit or root	List	organizationalunit (p. 1366)		
root (p. 1366)					
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 (p. 1366)		
organizationalunit (p. 1366)					
ListPolicies	Grants permission to list all of the policies in an organization	List			organizations:PolicyType (p. 1367)
ListPoliciesForTarget	Grants permission to list all of the policies that are directly attached to a root, organizational unit (OU), or account	List	account (p. 1366)		
	organizationalunit (p. 1366)				
	root (p. 1366)				
				organizations:PolicyType (p. 1367)	

Service Authorization Reference
Service Authorization Reference
AWS Organizations

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 (p. 1366)		
			organizationalunit (p. 1366)		
			policy (p. 1366)		
			root (p. 1366)		
ListTargetsForPolicy	Grants permission to list all the roots, OUs, and accounts to which a policy is attached	List	policy* (p. 1366)		
				organizations:PolicyType (p. 1367)	
MoveAccount	Grants permission to move an account from its current root or OU to another parent root or OU	Write	account* (p. 1366)		
			organizationalunit (p. 1366)		
RegisterDelegatedMember	Grants permission to register the specified member account to administer the Organizations features of the AWS service that is specified by ServicePrincipal	Write	account* (p. 1366)		
				organizations:ServicePrincipal (p. 1367)	
RemoveAccountFromOrganization	Grants permission to remove the specified account from the organization	Write	account* (p. 1366)		
TagResource	Grants permission to add one or more tags to the specified resource	Tagging	account (p. 1366)		
			organizationalunit (p. 1366)		
			policy (p. 1366)		
			root (p. 1366)		
				aws:TagKeys (p. 1367)	
				aws:RequestTag/ \${TagKey} (p. 1367)	
UntagResource	Grants permission to remove one or more tags from the specified resource	Tagging	account (p. 1366)		
			organizationalunit (p. 1366)		
			policy (p. 1366)		
			root (p. 1366)		
				aws:TagKeys (p. 1367)	
UpdateOrganization	Grants permission to rename an organizational unit (OU)	Write	organizationalunit* (p. 1366)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdatePolicy	Grants permission to update an existing policy with a new name, description, or content	Write	policy* (p. 1366)		
				organizations:PolicyType (p. 1367)	

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 \(p. 1360\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
account	arn:\${Partition}:organizations::\${MasterAccountId}:account/o-\${OrganizationId}/\${AccountId}	aws:ResourceTag/\${TagKey} (p. 1367)
handshake	arn:\${Partition}:organizations::\${MasterAccountId}:handshake/o-\${OrganizationId}/\${HandshakeType}/h-\${HandshakeId}	
organization	arn:\${Partition}:organizations::\${MasterAccountId}:organization/o-\${OrganizationId}	
organizationalunit	arn:\${Partition}:organizations::\${MasterAccountId}:ou/o-\${OrganizationId}/ou-\${OrganizationalUnitId}	aws:ResourceTag/\${TagKey} (p. 1367)
policy	arn:\${Partition}:organizations::\${MasterAccountId}:policy/o-\${OrganizationId}/\${PolicyType}/p-\${PolicyId}	aws:ResourceTag/\${TagKey} (p. 1367)
awspolicy	arn:\${Partition}:organizations::aws:policy/\${PolicyType}/p-\${PolicyId}	
root	arn:\${Partition}:organizations::\${MasterAccountId}:root/o-\${OrganizationId}/r-\${RootId}	aws:ResourceTag/\${TagKey} (p. 1367)

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters access by the tags that are passed in the request	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters access by the tags associated with the resource	String
<code>aws:TagKeys</code>	Filters access by the tag keys that are passed in the request	ArrayOfString
<code>organizations:PolicyType</code>	Filters access by the specified policy type names	String
<code>organizations:ServicePrincipal</code>	Filters access by the specified service principal 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 \(p. 1367\)](#)
- [Resource types defined by AWS Outposts \(p. 1369\)](#)
- [Condition keys for AWS Outposts \(p. 1369\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelOrder	Grants permission to cancel an order	Write			
CreateOrder	Grants permission to create an order	Write			
CreateOutpost	Grants permission to create an Outpost	Write			
CreatePrivateConnectivityConfig	Grants permission to create a private connectivity configuration	Write			
CreateSite	Grants permission to create a site	Write			
DeleteOutpost	Grants permission to delete an Outpost	Write			
DeleteSite	Grants permission to delete a site	Write			
GetCatalogItem	Grants permission to get a catalog item	Read			
GetOrder	Grants permission to get information about an order	Read			
GetOutpost	Grants permission to get information about the specified Outpost	Read			
GetOutpostInstanceTypes	Grants permission to get the instance types for the specified Outpost	Read			
GetPrivateConnectivityConfigInfo	Grants permission to get a private connectivity configuration	Read			
GetSite	Grants permission to get a site	Read			
GetSiteAddress	Grants permission to get a site address	Read			
ListAssets	Grants permission to list the assets for your Outpost	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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListSites	Grants permission to list the sites for your AWS account	List			
ListTagsForResource	Grants permission to list tags for a resource	Read			
TagResource	Grants permission to tag a resource	Tagging			
UntagResource	Grants permission to untag a resource	Tagging			
UpdateOutpost	Grants permission to update an Outpost	Write			
UpdateSite	Grants permission to update a site	Write			
UpdateSiteAddress	Grants permission to update the site address	Write			
UpdateSiteRackPhysicalProperties	Grants permission to update the physical properties of a rack at a site	Write			

Resource types defined by AWS Outposts

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

Condition keys for AWS Outposts

Outposts 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 [Available keys for conditions](#).

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 \(p. 1370\)](#)

- [Resource types defined by AWS Panorama \(p. 1376\)](#)
- [Condition keys for AWS Panorama \(p. 1376\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateApp [permission only]	Grants permission to create an AWS Panorama application	Write		aws:TagKeys (p. 1376) aws:RequestTag/\${TagKey} (p. 1376)	
CreateAppDeploy [permission only]	Grants permission to deploy an AWS Panorama application	Write			
CreateAppVersion [permission only]	Grants permission to create a version of an AWS Panorama application	Write	appVersion* (p. 1376)		
CreateApplication	Grants permission to create an AWS Panorama Application Instance	Write		aws:TagKeys (p. 1376) aws:RequestTag/\${TagKey} (p. 1376)	
CreateDataSource [permission only]	Grants permission to create an AWS Panorama datasource	Write	device* (p. 1376)		
				aws:TagKeys (p. 1376) aws:RequestTag/\${TagKey} (p. 1376)	
CreateDeployment [permission only]	Grants permission to configure a deployment for an AWS Panorama application	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateInputs [permission only]	Grants permission to generate a list of cameras on the same network as an AWS Panorama Appliance	Write	device* (p. 1376)		
CreateJobForDevice [permission only]	Grants permission to create a job for an AWS Panorama Appliance	Write			
CreateModel [permission only]	Grants permission to import a machine learning model into AWS Panorama	Write		aws:TagKeys (p. 1376) aws:RequestTag/\${TagKey} (p. 1376)	
CreateNodeFromTemplate	Grants permission to create an AWS Panorama Node	Write			
CreatePackage	Grants permission to create an AWS Panorama Package	Write		aws:TagKeys (p. 1376) aws:RequestTag/\${TagKey} (p. 1376)	
CreatePackageTemplate	Grants permission to create an AWS Panorama Package	Write			
CreateStreams [permission only]	Grants permission to generate a list of streams available to an AWS Panorama Appliance	Write	device* (p. 1376)		
DeleteApp [permission only]	Grants permission to delete an AWS Panorama application	Write	app* (p. 1376)		
DeleteAppVersion [permission only]	Grants permission to delete a version of an AWS Panorama application	Write	app* (p. 1376)		
DeleteDataSource [permission only]	Grants permission to delete an AWS Panorama datasource	Write	dataSource* (p. 1376)		
DeleteDevice [permission only]	Grants permission to deregister an AWS Panorama Appliance	Write	device* (p. 1376)		
DeleteModel [permission only]	Grants permission to delete a machine learning model from AWS Panorama	Write	model* (p. 1376)		
DeletePackage	Grants permission to delete an AWS Panorama Package	Write	package* (p. 1376)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeregisterPackage [permission only]	Grants permission to deregister an AWS Panorama Package Version	Write			
DescribeApp [permission only]	Grants permission to view details about an AWS Panorama application	Read	app* (p. 1376)		
DescribeAppDeployment [permission only]	Grants permission to view details about a deployment for an AWS Panorama application	Read			
DescribeAppVersion [permission only]	Grants permission to view details about a version of an AWS Panorama application	Read	app* (p. 1376)		
DescribeApplication [permission only]	Grants permission to view details about an AWS Panorama Application Instance	Read	applicationInstance* (p. 1376)		
DescribeApplicationDetail [permission only]	Grants permission to view details about an AWS Panorama Application Instance	Read	applicationInstance* (p. 1376)		
DescribeDataSource [permission only]	Grants permission to view details about a datasource in AWS Panorama	Read	dataSource* (p. 1376)		
DescribeDevice [permission only]	Grants permission to view details about an AWS Panorama Appliance	Read	device* (p. 1376)		
DescribeDeviceJob [permission only]	Grants permission to view job details for an AWS Panorama Appliance	Read			
DescribeModel [permission only]	Grants permission to view details about a machine learning model in AWS Panorama	Read	model* (p. 1376)		
DescribeNode	Grants permission to view details about an AWS Panorama Node	Read			
DescribeNodeFromJob	Grants permission to view details about an AWS Panorama 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* (p. 1376)		
DescribePackageDetails	Grants permission to view details about an AWS Panorama Package	Read			
DescribePackageVersionDetails	Grants permission to view details about an AWS Panorama Package Version	Read			
DescribeSoftware [permission only]	Grants permission to view details about a software version for the AWS Panorama Appliance	Read			
GetDeploymentConfiguration [permission only]	Grants permission to view details about a deployment configuration for an AWS Panorama application	Read			
GetInputs [permission only]	Grants permission to retrieve a list of cameras generated with CreateInputs	Read	device* (p. 1376)		
GetStreams [permission only]	Grants permission to retrieve a list of streams generated with CreateStreams	Read	device* (p. 1376)		
GetWebSocketURL [permission only]	Grants permission to generate a WebSocket endpoint for communication with AWS Panorama	Read			
ListAppDeployments [permission only]	Grants permission to retrieve a list of deployments for an AWS Panorama application	List			
ListAppVersions [permission only]	Grants permission to retrieve a list of application versions in AWS Panorama	List	app* (p. 1376)		
ListApplicationInstances	Grants permission to retrieve a list of application instance dependencies in AWS Panorama	List			
ListApplicationInstanceModels	Grants permission to retrieve a list of model instances of application instances in AWS Panorama	List			

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			
ListApps [permission only]	Grants permission to retrieve a list of applications in AWS Panorama	List			
ListDataSources [permission only]	Grants permission to retrieve a list of datasources in AWS Panorama	List	device* (p. 1376)		
ListDeploymentConfigurations [permission only]	Grants permission to retrieve a list of deployment configurations in AWS Panorama	List			
ListDevices [permission only]	Grants permission to retrieve a list of appliances in AWS Panorama	List			
ListDevicesJobs [permission only]	Grants permission to retrieve a list of jobs for an AWS Panorama Appliance	List			
ListModels [permission only]	Grants permission to retrieve a list of models in AWS Panorama	List			
ListNodeFromTemplate	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			
ListPackageImports	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 [permission only]	Grants permission to retrieve a list of tags for a resource in AWS Panorama	Read	app (p. 1376)		
dataSource (p. 1376)					
device (p. 1376)					
model (p. 1376)					

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ProvisionDevice [permission only]	Grants permission to register an AWS Panorama Appliance	Write		aws:TagKeys (p. 1376) aws:RequestTag/ \${TagKey} (p. 1376)	
RegisterPackage	Grants permission to register an AWS Panorama Package Version	Write			
RemoveApplication	Grants permission to remove an AWS Panorama Application Instance	Write	applicationInstance* (p. 1376)		
TagResource [permission only]	Grants permission to add tags to a resource in AWS Panorama	Tagging	app (p. 1376)		
dataSource (p. 1376)					
device (p. 1376)					
model (p. 1376)					
aws:TagKeys (p. 1376)					
UntagResource [permission only]	Grants permission to remove tags from a resource in AWS Panorama	Tagging	app (p. 1376)		
dataSource (p. 1376)					
device (p. 1376)					
model (p. 1376)					
aws:TagKeys (p. 1376)					
UpdateApp [permission only]	Grants permission to modify an AWS Panorama application	Write	app* (p. 1376)		
UpdateAppConfig [permission only]	Grants permission to modify the version-specific configuration of an AWS Panorama application	Write	app* (p. 1376)		
UpdateDataSource [permission only]	Grants permission to modify an AWS Panorama datasource	Write	dataSource* (p. 1376)		
UpdateDeviceMetadata [permission only]	Grants permission to modify basic settings for an AWS Panorama Appliance	Write			

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 \(p. 1370\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
device	<code>arn:\${Partition}:panorama:\${Region}: \${Account}:device/\${DeviceId}</code>	aws:ResourceTag/\${TagKey} (p. 1376)
package	<code>arn:\${Partition}:panorama:\${Region}: \${Account}:package/\${PackageId}</code>	aws:ResourceTag/\${TagKey} (p. 1376)
applicationInstance	<code>arn:\${Partition}:panorama:\${Region}: \${Account}:applicationInstance/ \${ApplicationInstanceId}</code>	aws:ResourceTag/\${TagKey} (p. 1376)
dataSource	<code>arn:\${Partition}:panorama:\${Region}: \${Account}:dataSource/\${DeviceId}/ \${DataSourceName}</code>	aws:ResourceTag/\${TagKey} (p. 1376)
model	<code>arn:\${Partition}:panorama:\${Region}: \${Account}:model/\${ModelName}</code>	aws:ResourceTag/\${TagKey} (p. 1376)
app	<code>arn:\${Partition}:panorama:\${Region}: \${Account}:app/\${AppName}</code>	aws:ResourceTag/\${TagKey} (p. 1376)
appVersion	<code>arn:\${Partition}:panorama:\${Region}: \${Account}:app/\${AppName}:\${AppVersion}</code>	

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters access by the tags that are passed in the request	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters access by the tags associated with the resource	String
<code>aws:TagKeys</code>	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 \(p. 1377\)](#)
- [Resource types defined by AWS Performance Insights \(p. 1378\)](#)
- [Condition keys for AWS Performance Insights \(p. 1378\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDimensions	Grants permission to call <code>DescribeDimensions</code> API to retrieve the top N dimension keys for a metric for a specific time period	Read	metric-resource* (p. 1378)		
GetDimensionKey	Grants permission to call <code>GetDimensionKey</code> API to retrieve the attributes of the specified dimension group	Read	metric-resource* (p. 1378)		
GetResourceMetadata	Grants permission to call <code>GetResourceMetadata</code> API	Read	metric-resource* (p. 1378)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	to retrieve the metadata for different features				
GetResourceMetrics	Grants permission to call GetResourceMetrics API to retrieve PI metrics for a set of data sources, over a time period	Read	metric-resource* (p. 1378)		
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* (p. 1378)		
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* (p. 1378)		

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 \(p. 1377\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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}	

Condition keys for AWS Performance Insights

Performance Insights 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 [Available keys for conditions](#).

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 \(p. 1379\)](#)
- [Resource types defined by Amazon Personalize \(p. 1383\)](#)
- [Condition keys for Amazon Personalize \(p. 1384\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1383)		
CreateBatchSegmentJob	Grants permission to create a batch segment job	Write	batchSegmentJob* (p. 1383)		
CreateCampaign	Grants permission to create a campaign	Write	campaign* (p. 1383)		
CreateDataset	Grants permission to create a dataset	Write	dataset* (p. 1383)		
CreateDatasetExportJob	Grants permission to create a dataset export job	Write	datasetExportJob* (p. 1383)		
CreateDatasetGroup	Grants permission to create a dataset group	Write	datasetGroup* (p. 1383)		
CreateDatasetImportJob	Grants permission to create a dataset import job	Write	datasetImportJob* (p. 1383)		
CreateEventTracker	Grants permission to create an event tracker	Write	eventTracker* (p. 1383)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateFilter	Grants permission to create a filter	Write	filter* (p. 1383)		
CreateRecommendation	Grants permission to create a recommender	Write	recommender* (p. 1383)		
CreateSchema	Grants permission to create a schema	Write	schema* (p. 1383)		
CreateSolution	Grants permission to create a solution	Write	solution* (p. 1383)		
CreateSolutionVersion	Grants permission to create a solution version	Write	solution* (p. 1383)		
DeleteCampaign	Grants permission to delete a campaign	Write	campaign* (p. 1383)		
DeleteDataset	Grants permission to delete a dataset	Write	dataset* (p. 1383)		
DeleteDatasetGroup	Grants permission to delete a dataset group	Write	datasetGroup* (p. 1383)		
DeleteEventTracker	Grants permission to delete an event tracker	Write	eventTracker* (p. 1383)		
DeleteFilter	Grants permission to delete a filter	Write	filter* (p. 1383)		
DeleteRecommender	Grants permission to delete a recommender	Write	recommender* (p. 1383)		
DeleteSchema	Grants permission to delete a schema	Write	schema* (p. 1383)		
DeleteSolution	Grants permission to delete a solution including all versions of the solution	Write	solution* (p. 1383)		
DescribeAlgorithm	Grants permission to describe an algorithm	Read	algorithm* (p. 1383)		
DescribeBatchInference	Grants permission to describe a batch inference job	Read	batchInferenceJob* (p. 1383)		
DescribeBatchSegment	Grants permission to describe a batch segment job	Read	batchSegmentJob* (p. 1383)		
DescribeCampaign	Grants permission to describe a campaign	Read	campaign* (p. 1383)		
DescribeDataset	Grants permission to describe a dataset	Read	dataset* (p. 1383)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDatasetExportJob	Grants permission to describe a dataset export job	Read	datasetExportJob* (p. 1383)		
DescribeDatasetGroup	Grants permission to describe a dataset group	Read	datasetGroup* (p. 1383)		
DescribeDatasetImportJob	Grants permission to describe a dataset import job	Read	datasetImportJob* (p. 1383)		
DescribeEventTracker	Grants permission to describe an event tracker	Read	eventTracker* (p. 1383)		
DescribeFeatureTransformation	Grants permission to describe a feature transformation	Read	featureTransformation* (p. 1383)		
DescribeFilter	Grants permission to describe a filter	Read	filter* (p. 1383)		
DescribeRecipe	Grants permission to describe a recipe	Read	recipe* (p. 1383)		
DescribeRecommender	Grants permission to describe a recommender	Read	recommender* (p. 1383)		
DescribeSchema	Grants permission to describe a schema	Read	schema* (p. 1383)		
DescribeSolution	Grants permission to describe a solution	Read	solution* (p. 1383)		
DescribeSolutionVersion	Grants permission to describe a version of a solution	Read	solution* (p. 1383)		
GetPersonalizedRanking	Grants permission to get a re-ranked list of recommendations	Read	campaign* (p. 1383)		
GetRecommendations	Grants permission to get a list of recommendations from a campaign	Read	campaign* (p. 1383)		
GetSolutionMetrics	Grants permission to get metrics for a solution version	Read	solution* (p. 1383)		
ListBatchInferenceJobs	Grants permission to list batch inference jobs	List			
ListBatchSegmentJobs	Grants permission to list batch segment jobs	List			
ListCampaigns	Grants permission to list campaigns	List			
ListDatasetExportJobs	Grants permission to list dataset export jobs	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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			
PutEvents	Grants permission to put real time event data	Write	eventTracker* (p. 1383)		
PutItems	Grants permission to ingest Items data	Write	dataset* (p. 1383)		
PutUsers	Grants permission to ingest Users data	Write	dataset* (p. 1383)		
StartRecommender	Grants permission to start a recommender	Write	recommender* (p. 1383)		
StopRecommender	Grants permission to stop a recommender	Write	recommender* (p. 1383)		
StopSolutionVersion	Grants permission to stop a solution version creation	Write	solution* (p. 1383)		
UpdateCampaign	Grants permission to update a campaign	Write	campaign* (p. 1383)		
UpdateRecommender	Grants permission to update a recommender	Write	recommender* (p. 1383)		

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 \(p. 1379\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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}	
featureTransformer	arn:\${Partition}:personalize:\${Region}: \${Account}: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}	
datasetExportJob	arn:\${Partition}:personalize:\${Region}: \${Account}:dataset-export-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:\${Region}: \${Account}:recipe/\${ResourceId}	
algorithm	arn:\${Partition}:personalize:\${Region}: \${Account}: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}	

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 [Available keys for conditions](#).

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 \(p. 1384\)](#)
- [Resource types defined by Amazon Pinpoint \(p. 1395\)](#)
- [Condition keys for Amazon Pinpoint \(p. 1396\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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		aws:RequestTag/\${TagKey} (p. 1396) aws:TagKeys (p. 1396) aws:ResourceTag/\${TagKey} (p. 1396)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCampaign	Grants permission to create a campaign for an app	Write	apps* (p. 1395)		
	aws:RequestTag/ {\$TagKey} (p. 1396)				
	aws:TagKeys (p. 1396)				
CreateEmailTemplate	Grants permission to create an email template	Write		aws:RequestTag/ {\$TagKey} (p. 1396)	
	aws:TagKeys (p. 1396)			aws:ResourceTag/ {\$TagKey} (p. 1396)	
CreateExportJob	Grants permission to create an export job that exports endpoint definitions to Amazon S3	Write	apps* (p. 1395)		
CreateImportJob	Grants permission to import endpoint definitions from to create a segment	Write	apps* (p. 1395)		
CreateInAppTemplate	Grants permission to create an in-app message template	Write		aws:RequestTag/ {\$TagKey} (p. 1396)	
	aws:TagKeys (p. 1396)			aws:ResourceTag/ {\$TagKey} (p. 1396)	
CreateJourney	Grants permission to create a Journey for an app	Write	apps* (p. 1395)	aws:RequestTag/ {\$TagKey} (p. 1396)	
	aws:TagKeys (p. 1396)				
	aws:ResourceTag/ {\$TagKey} (p. 1396)				
CreatePushTemplate	Grants permission to create a push notification template	Write		aws:RequestTag/ {\$TagKey} (p. 1396)	
	aws:TagKeys (p. 1396)			aws:ResourceTag/ {\$TagKey} (p. 1396)	
CreateRecommendationConfiguration	Grants permission to create an Amazon Pinpoint configuration for a recommender model	Write			

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	apps* (p. 1395)	aws:RequestTag/\${TagKey} (p. 1396) aws:TagKeys (p. 1396) aws:ResourceTag/\${TagKey} (p. 1396)	
CreateSmsTemplate	Grants permission to create an SMS message template	Write		aws:RequestTag/\${TagKey} (p. 1396) aws:TagKeys (p. 1396) aws:ResourceTag/\${TagKey} (p. 1396)	
CreateVoiceTemplate	Grants permission to create a voice message template	Write		aws:RequestTag/\${TagKey} (p. 1396) aws:TagKeys (p. 1396) aws:ResourceTag/\${TagKey} (p. 1396)	
DeleteAdmChannel	Grants permission to delete the ADM channel for an app	Write	apps* (p. 1395)		
DeleteApnsChannel	Grants permission to delete the APNs channel for an app	Write	apps* (p. 1395)		
DeleteApnsSandboxChannel	Grants permission to delete the APNs sandbox channel for an app	Write	apps* (p. 1395)		
DeleteApnsVoipChannel	Grants permission to delete the APNs VoIP channel for an app	Write	apps* (p. 1395)		
DeleteApnsVoipSandboxChannel	Grants permission to delete the APNs VoIP sandbox channel for an app	Write	apps* (p. 1395)		
DeleteApp	Grants permission to delete a specific campaign	Write	apps* (p. 1395)		
DeleteBaiduChannel	Grants permission to delete the Baidu channel for an app	Write	apps* (p. 1395)		
DeleteCampaign	Grants permission to delete a specific campaign	Write	apps* (p. 1395)	campaigns* (p. 1395)	
DeleteEmailChannel	Grants permission to delete the Email channel for an app	Write	apps* (p. 1395)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteEmailTemplate	Grants permission to delete an email template or an email template version	Write	templates* (p. 1396)		
DeleteEndpoint	Grants permission to delete an endpoint	Write	apps* (p. 1395)		
DeleteEventStream	Grants permission to delete the event stream for an app	Write	apps* (p. 1395)		
DeleteGcmChannel	Grants permission to delete the GCM channel for an app	Write	apps* (p. 1395)		
DeleteInAppTemplate	Grants permission to delete an in-app message template or an in-app message template version	Write	templates* (p. 1396)		
DeleteJourney	Grants permission to delete a specific journey	Write	apps* (p. 1395)	journeys* (p. 1395)	
DeletePushTemplate	Grants permission to delete a push notification template or a push notification template version	Write	templates* (p. 1396)		
DeleteRecommender	Grants permission to delete an Amazon Pinpoint configuration for a recommender model	Write	recommenders* (p. 1396)		
DeleteSegment	Grants permission to delete a specific segment	Write	apps* (p. 1395)	segments* (p. 1395)	
DeleteSmsChannel	Grants permission to delete the SMS channel for an app	Write	apps* (p. 1395)		
DeleteSmsTemplate	Grants permission to delete an sms message template or an sms message template version	Write	templates* (p. 1396)		
DeleteUserEndpoint	Grants permission to delete all of the endpoints that are associated with a user ID	Write	apps* (p. 1395)		
DeleteVoiceChannel	Grants permission to delete the voice channel for an app	Write	apps* (p. 1395)		
DeleteVoiceTemplate	Grants permission to delete a voice message template or a voice message template version	Write	templates* (p. 1396)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAdmChannel	Grants permission to retrieve information about the Amazon Device Messaging (ADM) channel for an app	Read	apps* (p. 1395)		
GetApnsChannel	Grants permission to retrieve information about the APNs channel for an app	Read	apps* (p. 1395)		
GetApnsSandboxInformation	Grants permission to retrieve information about the APNs sandbox channel for an app	Read	apps* (p. 1395)		
GetApnsVoipChannelInformation	Grants permission to retrieve information about the APNs VoIP channel for an app	Read	apps* (p. 1395)		
GetApnsVoipSandboxInformation	Grants permission to retrieve information about the APNs VoIP sandbox channel for an app	Read	apps* (p. 1395)		
GetApp	Grants permission to retrieve information about a specific app in your Amazon Pinpoint account	Read	apps* (p. 1395)		
GetApplicationDataSeries	Grants permission to retrieve pre-aggregated data for a standard metric that applies to an application	Read	apps* (p. 1395)		
GetApplicationSettings	Grants permission to retrieve the default settings for an app	List	apps* (p. 1395)		
GetApps	Grants permission to retrieve a list of apps in your Amazon Pinpoint account	Read	apps* (p. 1395)		
GetBaiduChannel	Grants permission to retrieve information about the Baidu channel for an app	Read	apps* (p. 1395)		
GetCampaign	Grants permission to retrieve information about a specific campaign	Read	apps* (p. 1395)		
			campaigns* (p. 1395)		
GetCampaignActivities	Grants permission to retrieve information about the activities performed by a campaign	List	apps* (p. 1395)		
			campaigns* (p. 1395)		
GetCampaignDataSeries	Grants permission to retrieve pre-aggregated data for a standard metric that applies to a campaign	Read	apps* (p. 1395)		
			campaigns* (p. 1395)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCampaignVersion	Grants permission to retrieve information about a specific campaign version	Read	apps* (p. 1395)		
			campaigns* (p. 1395)		
GetCampaignVersions	Grants permission to retrieve information about the current and prior versions of a campaign	List	apps* (p. 1395)		
			campaigns* (p. 1395)		
GetCampaigns	Grants permission to retrieve information about all campaigns for an app	List	apps* (p. 1395)		
GetChannels	Grants permission to get all channels information for your app	List	apps* (p. 1395)		
GetEmailChannel	Grants permission to obtain information about the email channel in an app	Read	apps* (p. 1395)		
GetEmailTemplate	Grants permission to retrieve information about a specific or the active version of an email template	Read	templates* (p. 1396)		
GetEndpoint	Grants permission to retrieve information about a specific endpoint	Read	apps* (p. 1395)		
GetEventStream	Grants permission to retrieve information about the event stream for an app	Read	apps* (p. 1395)		
GetExportJob	Grants permission to obtain information about a specific export job	Read	apps* (p. 1395)		
GetExportJobs	Grants permission to retrieve a list of all of the export jobs for an app	List	apps* (p. 1395)		
GetGcmChannel	Grants permission to retrieve information about the GCM channel for an app	Read	apps* (p. 1395)		
GetImportJob	Grants permission to retrieve information about a specific import job	Read	apps* (p. 1395)		
GetImportJobs	Grants permission to retrieve information about all import jobs for an app	List	apps* (p. 1395)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetInAppMessage	Grants permission to retrieve in-app messages for the given endpoint id	Read	apps* (p. 1395)		
GetInAppTemplate	Grants permission to retrieve information about a specific or the active version of an in-app message template	Read	templates* (p. 1396)		
GetJourney	Grants permission to retrieve information about a specific journey	Read	apps* (p. 1395)		
			journeys* (p. 1395)		
GetJourneyDataReport	Grants permission to retrieve (queries) pre-aggregated data for a standard engagement metric that applies to a journey	Read	apps* (p. 1395)		
			journeys* (p. 1395)		
GetJourneyExecutionMetric	Grants permission to retrieve (queries) pre-aggregated data for a standard execution metric that applies to a journey activity	Read	apps* (p. 1395)		
			journeys* (p. 1395)		
GetJourneyExecutionMetric	Grants permission to retrieve (queries) pre-aggregated data for a standard execution metric that applies to a journey	Read	apps* (p. 1395)		
			journeys* (p. 1395)		
GetPushTemplate	Grants permission to retrieve information about a specific or the active version of an push notification template	Read	templates* (p. 1396)		
GetRecommenderInformation	Grants permission to retrieve information about an Amazon Pinpoint configuration for a recommender model	Read	recommenders* (p. 1396)		
GetRecommenderInformation	Grants permission to retrieve information about all the recommender model configurations that are associated with an Amazon Pinpoint account	List			
GetReports	Grants permission to mobiletargeting:GetReports	Read			
GetSegment	Grants permission to retrieve information about a specific segment	Read	apps* (p. 1395)		
			segments* (p. 1395)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSegmentExportInformation	Grants permission to retrieve information about jobs that export endpoint definitions from segments to Amazon S3	List	apps* (p. 1395)		
			segments* (p. 1395)		
GetSegmentImportInformation	Grants permission to retrieve information about jobs that create segments by importing endpoint definitions from	List	apps* (p. 1395)		
			segments* (p. 1395)		
GetSegmentVersionInformation	Grants permission to retrieve information about a specific segment version	Read	apps* (p. 1395)		
			segments* (p. 1395)		
GetSegmentVersionsInformation	Grants permission to retrieve information about the current and prior versions of a segment	List	apps* (p. 1395)		
			segments* (p. 1395)		
GetSegments	Grants permission to retrieve information about the segments for an app	List	apps* (p. 1395)		
GetSmsChannel	Grants permission to obtain information about the SMS channel in an app	Read	apps* (p. 1395)		
GetSmsTemplate	Grants permission to retrieve information about a specific or the active version of an sms message template	Read	templates* (p. 1396)		
 GetUserEndpoint	Grants permission to retrieve information about the endpoints that are associated with a user ID	Read	apps* (p. 1395)		
GetVoiceChannel	Grants permission to obtain information about the Voice channel in an app	Read	apps* (p. 1395)		
GetVoiceTemplate	Grants permission to retrieve information about a specific or the active version of a voice message template	Read	templates* (p. 1396)		
ListJourneys	Grants permission to retrieve information about all journeys for an app	List	apps* (p. 1395)		
ListTagsForResource	Grants permission to list tags for a resource	Read	apps (p. 1395)		
			campaigns (p. 1395)		
			segments (p. 1395)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTemplateVersions	Grants permission to retrieve all versions about a specific template	List	templates* (p. 1396)		
ListTemplates	Grants permission to retrieve metadata about the queried templates	List	templates* (p. 1396)		
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* (p. 1396)		
PutEventStream	Grants permission to create or update an event stream for an app	Write	apps* (p. 1395)		
PutEvents	Grants permission to create or update events for an app	Write	apps* (p. 1395)		
RemoveAttributes	Grants permission to remove the attributes for an app	Write	apps* (p. 1395)		
SendMessages	Grants permission to send an SMS message or push notification to specific endpoints	Write	apps* (p. 1395)		
SendOTPMessages	Grants permission to send an OTP code to a user of your application	Write	apps* (p. 1395)		
SendUsersMessages	Grants permission to send an SMS message or push notification to all endpoints that are associated with a specific user ID	Write	apps* (p. 1395)		
TagResource	Grants permission to add tags to a resource	Tagging	apps (p. 1395)		
			campaigns (p. 1395)		
			segments (p. 1395)		
			aws:RequestTag/\${TagKey} (p. 1396)		
			aws:TagKeys (p. 1396)		
UntagResource	Grants permission to remove tags from a resource	Tagging	apps (p. 1395)		
			campaigns (p. 1395)		
			segments (p. 1395)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 1396) aws:TagKeys (p. 1396)	
UpdateAdmChannel	Grants permission to update the Amazon Device Messaging (ADM) channel for an app	Write	apps* (p. 1395)		
UpdateApnsChannel	Grants permission to update the Apple Push Notification service (APNs) channel for an app	Write	apps* (p. 1395)		
UpdateApnsSandboxChannel	Grants permission to update the Apple Push Notification service (APNs) sandbox channel for an app	Write	apps* (p. 1395)		
UpdateApnsVoipChannel	Grants permission to update the Apple Push Notification service (APNs) VoIP channel for an app	Write	apps* (p. 1395)		
UpdateApnsVoipSandboxChannel	Grants permission to update the Apple Push Notification service (APNs) VoIP sandbox channel for an app	Write	apps* (p. 1395)		
UpdateApplicationDefaultSettings	Grants permission to update the application default settings for an app	Write	apps* (p. 1395)		
UpdateBaiduChannel	Grants permission to update the Baidu channel for an app	Write	apps* (p. 1395)		
UpdateCampaign	Grants permission to update a specific campaign	Write	apps* (p. 1395)		
			campaigns* (p. 1395)		
			aws:RequestTag/ \${TagKey} (p. 1396)		
			aws:TagKeys (p. 1396)		
UpdateEmailChannel	Grants permission to update the email channel for an app	Write	apps* (p. 1395)		
UpdateEmailTemplate	Grants permission to update a specific email template under the same version or generate a new version	Write	templates* (p. 1396)		
			aws:RequestTag/ \${TagKey} (p. 1396)		
UpdateEndpoint	Grants permission to create an endpoint or update the information for an endpoint	Write	apps* (p. 1395)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateEndpointsBatch	Grants permission to create or update endpoints as a batch operation	Write	apps* (p. 1395)		
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	apps* (p. 1395)		
UpdateInAppTemplate	Grants permission to update a specific in-app message template under the same version or generate a new version	Write	templates* (p. 1396)		
UpdateJourney	Grants permission to update a specific journey	Write	apps* (p. 1395)		
			journeys* (p. 1395)		
				aws:RequestTag/ \${TagKey} (p. 1396)	
UpdateJourneyState	Grants permission to update a specific journey state	Write	apps* (p. 1395)		
journeys* (p. 1395)					
	aws:RequestTag/ \${TagKey} (p. 1396)				
UpdatePushTemplate	Grants permission to update a specific push notification template under the same version or generate a new version	Write	templates* (p. 1396)		
	aws:RequestTag/ \${TagKey} (p. 1396)				
	aws:TagKeys (p. 1396)				
UpdateRecommender	Grants permission to update an Amazon Pinpoint configuration for a recommender model	Write	recommenders* (p. 1396)		
UpdateSegment	Grants permission to update a specific segment	Write	apps* (p. 1395)		
	segments* (p. 1395)				
	aws:RequestTag/ \${TagKey} (p. 1396)				
	aws:TagKeys (p. 1396)				

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateSmsChannel	Grants permission to update the SMS channel for an app	Write	apps* (p. 1395)		
UpdateSmsTemplate	Grants permission to update a specific sms message template under the same version or generate a new version	Write	templates* (p. 1396)		
				aws:RequestTag/ \${TagKey} (p. 1396) aws:TagKeys (p. 1396)	
UpdateTemplateActiveVersion	Grants permission to update the ActiveVersion parameter of a specific template	Write	templates* (p. 1396)		
UpdateVoiceChannel	Grants permission to update the Voice channel for an app	Write	apps* (p. 1395)		
UpdateVoiceTemplate	Grants permission to update a specific voice message template under the same version or generate a new version	Write	templates* (p. 1396)		
				aws:RequestTag/ \${TagKey} (p. 1396) aws:TagKeys (p. 1396)	
VerifyOTPMessages	Grants permission to check the validity of One-Time Passwords (OTPs)	Write	apps* (p. 1395)		

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 \(p. 1384\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
apps	arn:\${Partition}:mobiletargeting:\${Region}: \${Account}:apps/\${AppId}	aws:ResourceTag/ \${TagKey} (p. 1396)
campaigns	arn:\${Partition}:mobiletargeting:\${Region}: \${Account}:apps/\${AppId}/campaigns/ \${CampaignId}	aws:ResourceTag/ \${TagKey} (p. 1396)
journeys	arn:\${Partition}:mobiletargeting:\${Region}: \${Account}:apps/\${AppId}/journeys/ \${JourneyId}	aws:ResourceTag/ \${TagKey} (p. 1396)
segments	arn:\${Partition}:mobiletargeting:\${Region}: \${Account}:apps/\${AppId}/segments/ \${SegmentId}	aws:ResourceTag/ \${TagKey} (p. 1396)

Resource types	ARN	Condition keys
templates	arn:\${Partition}:mobiletargeting:\${Region}: \${Account}:templates/\${TemplateName}/ \${ChannelType}	aws:ResourceTag/\${TagKey} (p. 1396)
recommenders	arn:\${Partition}:mobiletargeting:\${Region}: \${Account}:recommenders/\${RecommenderId}	
phone-number-validate	arn:\${Partition}:mobiletargeting:\${Region}: \${Account}:phone/number/validate	

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 [Available global condition 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
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 \(p. 1397\)](#)
- [Resource types defined by Amazon Pinpoint Email Service \(p. 1403\)](#)
- [Condition keys for Amazon Pinpoint Email Service \(p. 1403\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 (p. 1403) aws:TagKeys (p. 1403) aws:RequestTag/\${TagKey} (p. 1403)	
CreateConfigurationSetEventDestination	Grants permission to create a configuration set event destination	Write	configuration-set* (p. 1403)	ses:ApiVersion (p. 1403) aws:ResourceTag/\${TagKey} (p. 1403)	
CreateDedicatedIpPool	Grants permission to create a pool of dedicated IP addresses	Write		ses:ApiVersion (p. 1403) aws:TagKeys (p. 1403) aws:RequestTag/\${TagKey} (p. 1403)	
CreateDeliverabilityTestPredictiveInboxPlacementTest	Grants permission to create a predictive inbox placement test	Write	identity* (p. 1403)	ses:ApiVersion (p. 1403) aws:TagKeys (p. 1403) aws:RequestTag/\${TagKey} (p. 1403)	
CreateEmailIdentityVerificationProcess	Grants permission to start the process of verifying an email identity	Write		ses:ApiVersion (p. 1403) aws:TagKeys (p. 1403) aws:RequestTag/\${TagKey} (p. 1403)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteConfigurationSet	Grants permission to delete an existing configuration set	Write	configuration-set* (p. 1403)		
			ses:ApiVersion (p. 1403) aws:ResourceTag/ {\$TagKey} (p. 1403)		
DeleteConfigurationSetDestinations	Grants permission to delete an event destination	Write	configuration-set* (p. 1403)		
			ses:ApiVersion (p. 1403) aws:ResourceTag/ {\$TagKey} (p. 1403)		
DeleteDedicatedIpPool	Grants permission to delete a dedicated IP pool	Write	dedicated-ip-pool* (p. 1403)		
			ses:ApiVersion (p. 1403) aws:ResourceTag/ {\$TagKey} (p. 1403)		
DeleteEmailIdentity	Grants permission to delete an email identity that you previously verified	Write	identity* (p. 1403)		
			ses:ApiVersion (p. 1403) aws:ResourceTag/ {\$TagKey} (p. 1403)		
GetAccount	Grants permission to get information about the email-sending status and capabilities	Read		ses:ApiVersion (p. 1403)	
GetBlacklistReport	Grants permission to retrieve a list of the deny lists on which your dedicated IP addresses appear	Read		ses:ApiVersion (p. 1403)	
GetConfigurationSet	Grants permission to get information about an existing configuration set	Read	configuration-set* (p. 1403)		
			ses:ApiVersion (p. 1403) aws:ResourceTag/ {\$TagKey} (p. 1403)		
GetConfigurationSetDestinations	Grants permission to retrieve destinations that are associated with a configuration set	Read	configuration-set* (p. 1403)		
			ses:ApiVersion (p. 1403) aws:ResourceTag/ {\$TagKey} (p. 1403)		

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 (p. 1403)	
GetDedicatedIps	Grants permission to list the dedicated IP addresses that are associated with your account	Read	dedicated-ip-pool* (p. 1403)		
			ses:ApiVersion (p. 1403)	aws:ResourceTag/\${TagKey} (p. 1403)	
GetDeliverabilityDashboard	Grants permission to get the status of the Deliverability dashboard	Read		ses:ApiVersion (p. 1403)	
GetDeliverabilityTestResults	Grants permission to retrieve the results of a predictive inbox placement test	Read	deliverability-test-report* (p. 1403)		
			ses:ApiVersion (p. 1403)	aws:ResourceTag/\${TagKey} (p. 1403)	
GetDomainDeliveryDetails	Grants permission to retrieve all the deliverability data for a specific campaign	Read		ses:ApiVersion (p. 1403)	
GetDomainStatistics	Grants permission to retrieve inbox placement and engagement rates for the domains that you use to send email	Read	identity* (p. 1403)		
			ses:ApiVersion (p. 1403)	aws:ResourceTag/\${TagKey} (p. 1403)	
GetEmailIdentity	Grants permission to get information about a specific identity associated with your account	Read	identity* (p. 1403)		
			ses:ApiVersion (p. 1403)	aws:ResourceTag/\${TagKey} (p. 1403)	
ListConfigurations	Grants permission to list all of the configuration sets associated with your account	List		ses:ApiVersion (p. 1403)	
ListDedicatedIpPools	Grants permission to list all of the dedicated IP pools that exist in your account	List		ses:ApiVersion (p. 1403)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDeliverabilityTests	Grants permission to retrieve a list of the predictive inbox placement tests that you've performed, regardless of their statuses	List		ses:ApiVersion (p. 1403)	
ListDomainDeliverabilityData	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 (p. 1403)	
ListEmailIdentities	Grants permission to list all of the email identities that are associated with your account	List		ses:ApiVersion (p. 1403)	
ListTagsForResource	Grants permission to retrieve a list of the tags (keys and values) that are associated with a specific resource	Read	configuration-set (p. 1403)		
			dedicated-ip-pool (p. 1403)		
			deliverability-test-report (p. 1403)		
			identity (p. 1403)		
				ses:ApiVersion (p. 1403)	
PutAccountDedicatedIp暖启动	Grants permission to enable or disable the automatic warm-up feature for dedicated IP addresses	Write		ses:ApiVersion (p. 1403)	
PutAccountSendingEnabled	Grants permission to enable or disable the ability of your account to send email	Write		ses:ApiVersion (p. 1403)	
PutConfigurationSetOptions	Grants permission to associate configuration sets with a dedicated IP pool	Write	configuration-set* (p. 1403)		
				ses:ApiVersion (p. 1403)	
				aws:ResourceTag/\${TagKey} (p. 1403)	
PutConfigurationSetReputationMetricsCollectionOption	Grants permission to enable or disable collection of reputation metrics for emails that you send using a particular configuration set	Write	configuration-set* (p. 1403)		
				ses:ApiVersion (p. 1403)	aws:ResourceTag/\${TagKey} (p. 1403)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutConfigurationSetDeliveryEnabled	Grants permission to enable or disable Email sending for messages that use a particular configuration set	Write	configuration-set* (p. 1403)		
			ses:ApiVersion (p. 1403) aws:ResourceTag/\${TagKey} (p. 1403)		
PutConfigurationSetCustomDomainName	Grants permission to specify a Custom domain name for open and click tracking elements in email that you send using a particular configuration set	Write	configuration-set* (p. 1403)		
			ses:ApiVersion (p. 1403) aws:ResourceTag/\${TagKey} (p. 1403)		
PutDedicatedIpPool	Grants permission to move a Dedicated IP address to an existing dedicated IP pool	Write	dedicated-ip-pool* (p. 1403)		
			ses:ApiVersion (p. 1403) aws:ResourceTag/\${TagKey} (p. 1403)		
PutDedicatedIpWarmUp	Grants permission to enable Dedicated IP warm up attributes	Write		ses:ApiVersion (p. 1403)	
PutDeliverabilityDashboard	Grants permission to enable Deliverability dashboard	Write		ses:ApiVersion (p. 1403)	
PutEmailIdentityDKIMAuthentication	Grants permission to enable or disable DKIM authentication for an email identity	Write	identity* (p. 1403)		
			ses:ApiVersion (p. 1403) aws:ResourceTag/\${TagKey} (p. 1403)		
PutEmailIdentityFeedbackForwarding	Grants permission to enable or disable Feedback forwarding for an identity	Write	identity* (p. 1403)		
			ses:ApiVersion (p. 1403) aws:ResourceTag/\${TagKey} (p. 1403)		
PutEmailIdentityMailFrom	Grants permission to enable or disable the custom MAIL FROM domain configuration for an email identity	Write	identity* (p. 1403)		
			ses:ApiVersion (p. 1403) aws:ResourceTag/\${TagKey} (p. 1403)		
SendEmail	Grants permission to send an email message	Write	identity* (p. 1403)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ses:ApiVersion (p. 1403) ses:FeedbackAddress (p. 1403) ses:FromAddress (p. 1403) ses:FromDisplayName (p. 1403) ses:Recipients (p. 1404)
TagResource	Grants permission to add one or more tags (keys and values) to a specified resource	Tagging	configuration-set (p. 1403)		
dedicated-ip-pool (p. 1403)					
deliverability-test-report (p. 1403)					
identity (p. 1403)					
	ses:ApiVersion (p. 1403) aws:TagKeys (p. 1403) aws:RequestTag/\${TagKey} (p. 1403)				
UntagResource	Grants permission to remove one or more tags (keys and values) from a specified resource	Tagging	configuration-set (p. 1403)		
dedicated-ip-pool (p. 1403)					
deliverability-test-report (p. 1403)					
identity (p. 1403)					
	ses:ApiVersion (p. 1403) aws:TagKeys (p. 1403)				
UpdateConfigurationSet*	Grants permission to update the configuration of an event destination for a configuration set	Write	configuration-set* (p. 1403)		
	ses:ApiVersion (p. 1403) aws:ResourceTag/\${TagKey} (p. 1403)				

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 \(p. 1397\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
configuration-set	<code>arn:\${Partition}:ses:\${Region}: \${Account}:configuration-set/ \${ConfigurationSetName}</code>	aws:ResourceTag/\${TagKey} (p. 1403)
dedicated-ip-pool	<code>arn:\${Partition}:ses:\${Region}: \${Account}:dedicated-ip-pool/ \${DedicatedIPPool}</code>	aws:ResourceTag/\${TagKey} (p. 1403)
deliverability-test-report	<code>arn:\${Partition}:ses:\${Region}: \${Account}:deliverability-test-report/ \${ReportId}</code>	aws:ResourceTag/\${TagKey} (p. 1403)
identity	<code>arn:\${Partition}:ses:\${Region}: \${Account}:identity/\${IdentityName}</code>	aws:ResourceTag/\${TagKey} (p. 1403)

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters actions based on the presence of tag key-value pairs in the request	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters actions based on tag key-value pairs attached to the resource	String
<code>aws:TagKeys</code>	Filters actions based on the presence of tag keys in the request	ArrayOfString
<code>ses:ApiVersion</code>	Filters actions based on the SES API version	String
<code>ses:FeedbackAddress</code>	Filters actions based on the "Return-Path" address, which specifies where bounces and complaints are sent by email feedback forwarding	String
<code>ses:FromAddress</code>	Filters actions based on the "From" address of a message	String
<code>ses:FromDisplayName</code>	Filters actions based on the "From" address that is used as the display name of a message	String

Condition keys	Description	Type
ses:Recipients	Filters actions based on the recipient addresses of a message, which include the "To", "CC", and "BCC" addresses	ArrayOfString

Actions, resources, and condition keys for Amazon 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 \(p. 1404\)](#)
- [Resource types defined by Amazon Pinpoint SMS and Voice Service \(p. 1405\)](#)
- [Condition keys for Amazon Pinpoint SMS and Voice Service \(p. 1405\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteConfigurationSet	Deletes an existing configuration set.	Write			
DeleteConfigurationDestination	Deletes an event destination in a configuration set.	Write			
GetConfigurationEventDestination	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 account in the current AWS Region.	Read			
SendVoiceMessage	Create a new voice message and send it to a recipient's phone number.	Write			
UpdateConfigurationDestination	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 [Available keys for conditions](#).

Actions, resources, and condition keys for Amazon Pinpoint SMS Voice V2

Amazon Pinpoint SMS 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 Amazon Pinpoint SMS Voice V2 \(p. 1406\)](#)
- [Resource types defined by Amazon Pinpoint SMS Voice V2 \(p. 1410\)](#)
- [Condition keys for Amazon Pinpoint SMS Voice V2 \(p. 1411\)](#)

Actions defined by Amazon Pinpoint SMS 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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateOriginationPhoneNumber	Grants permission to associate an origination phone number or sender ID to a pool	Write	Pool* (p. 1410)		
			PhoneNumber (p. 1410)		
			SenderId (p. 1410)		
CreateConfigurationSet	Grants permission to create a configuration set	Write		aws:RequestTag-\${TagKey} (p. 1411) aws:TagKeys (p. 1411)	TagResource
CreateEventDestination	Grants permission to create an event destination within a configuration set	Write	ConfigurationSet* (p. 1410)	iam:PassRole	
CreateOptOutList	Grants permission to create an opt-out list	Write		aws:RequestTag-\${TagKey} (p. 1411) aws:TagKeys (p. 1411)	TagResource
CreatePool	Grants permission to create a pool	Write	PhoneNumber (p. 1410)	sms-voice:TagResource	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			SenderId (p. 1410)		
			aws:RequestTag/ \${TagKey} (p. 1411)		aws:TagKeys (p. 1411)
DeleteConfigurationSet	Grants permission to delete a configuration set	Write	ConfigurationSet* (p. 1410)		
DeleteDefaultMessageType	Grants permission to delete the default message type for a configuration set	Write	ConfigurationSet* (p. 1410)		
DeleteDefaultSenderId	Grants permission to delete the default sender ID for a configuration set	Write	ConfigurationSet* (p. 1410)		
DeleteEventDestination	Grants permission to delete an event destination within a configuration set	Write	ConfigurationSet* (p. 1410)		
DeleteKeyword	Grants permission to delete a keyword for a pool or origination phone number	Write	PhoneNumber (p. 1410)		
			Pool (p. 1410)		
DeleteOptOutList	Grants permission to delete an opt-out list	Write	OptOutList* (p. 1410)		
DeleteOptedOutPhoneNumber	Grants permission to delete a destination phone number from an opt-out list	Write	OptOutList* (p. 1410)		
DeletePool	Grants permission to delete a pool	Write	Pool* (p. 1410)		
DeleteTextMessageOverride	Grants permission to delete an override for your account's text messaging monthly spend limit	Write			
DeleteVoiceMessageOverride	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			
DescribeAccountServiceQuotas	Grants permission to describe the service quotas for your account	Read			
DescribeConfigurationSets	Grants permission to describe the configuration sets in your account	Read	ConfigurationSet (p. 1410)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeKeywords	Grants permission to describe the keywords for a pool or origination phone number	Read	PhoneNumber (p. 1410)		
			Pool (p. 1410)		
DescribeOptOutList	Grants permission to describe the opt-out lists in your account	Read	OptOutList (p. 1410)		
DescribeOptedOutNumbers	Grants permission to describe the destination phone numbers in an opt-out list	Read	OptOutList* (p. 1410)		
DescribePhoneNumbers	Grants permission to describe the origination phone numbers in your account	Read	PhoneNumber (p. 1410)		
DescribePools	Grants permission to describe the pools in your account	Read	Pool (p. 1410)		
DescribeSenderId	Grants permission to describe the sender IDs in your account	Read	SenderId (p. 1410)		
DescribeSpendLimits	Grants permission to describe the monthly spend limits for your account	Read			
DisassociateOriginationNumber	Grants permission to dissociate an origination phone number or sender ID from a pool	Write	Pool* (p. 1410)		
			PhoneNumber (p. 1410)		
			SenderId (p. 1410)		
ListPoolOriginationNumbers	Grants permission to list all origination phone numbers and sender IDs associated to a pool	Read	Pool* (p. 1410)		
ListTagsForResource	Grants permission to list the tags for a resource	Read	ConfigurationSet (p. 1410)		
			OptOutList (p. 1410)		
			PhoneNumber (p. 1410)		
			Pool (p. 1410)		
			SenderId (p. 1410)		
PutKeyword	Grants permission to create or update a keyword for a pool or origination phone number	Write	PhoneNumber (p. 1410)		
			Pool (p. 1410)		
PutOptedOutNumber	Grants permission to put a destination phone number into an opt-out list	Write	OptOutList* (p. 1410)		
ReleasePhoneNumber	Grants permission to release an origination phone number	Write	PhoneNumber* (p. 1410)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RequestPhoneNumbers	Grants permission to request an origination phone number	Write	Pool (p. 1410)		sms-voice:AssociateOrigination sms-voice:TagResource
			aws:RequestTag/\${TagKey} (p. 1411) aws:TagKeys (p. 1411)		
SendTextMessage	Grants permission to send a text message to a destination phone number	Write	PhoneNumber (p. 1410)		
			Pool (p. 1410)		
			SenderId (p. 1410)		
SendVoiceMessage	Grants permission to send a voice message to a destination phone number	Write	PhoneNumber (p. 1410)		
			Pool (p. 1410)		
SetDefaultMessageType	Grants permission to set the default message type for a configuration set	Write	ConfigurationSet* (p. 1410)		
SetDefaultSenderId	Grants permission to set the default sender ID for a configuration set	Write	ConfigurationSet* (p. 1410)		
SetTextMessageSpendOverride	Grants permission to set an override for your account's text messaging monthly spend limit	Write			
SetVoiceMessageSpendOverride	Grants permission to set an override for your account's voice messaging monthly spend limit	Write			
TagResource	Grants permission to add tags to a resource	Tagging	ConfigurationSet (p. 1410)		
OptOutList (p. 1410)					
PhoneNumber (p. 1410)					
Pool (p. 1410)					
SenderId (p. 1410)					
aws:RequestTag/\${TagKey} (p. 1411) aws:TagKeys (p. 1411)					
UntagResource	Grants permission to remove tags from a resource	Tagging	ConfigurationSet (p. 1410)		
OptOutList (p. 1410)					
PhoneNumber (p. 1410)					

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Pool (p. 1410)		
			SenderId (p. 1410)		
			aws:RequestTag/ \${TagKey} (p. 1411)	aws:TagKeys (p. 1411)	
UpdateEventDestination	Grants permission to update an event destination within a configuration set	Write	ConfigurationSet* (p. 1410)	iam:PassRole	
UpdatePhoneNumber	Grants permission to update a destination phone number's configuration	Write	PhoneNumber* (p. 1410)		
UpdatePool	Grants permission to update a pool's configuration	Write	Pool* (p. 1410)		

Resource types defined by Amazon Pinpoint SMS 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 \(p. 1406\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1411)
OptOutList	arn:\${Partition}:sms-voice:\${Region}: \${Account}:opt-out-list/\${OptOutListName}	aws:ResourceTag/ \${TagKey} (p. 1411)
PhoneNumber	arn:\${Partition}:sms-voice:\${Region}: \${Account}:phone-number/\${PhoneNumberId}	aws:ResourceTag/ \${TagKey} (p. 1411)
Pool	arn:\${Partition}:sms-voice:\${Region}: \${Account}:pool/\${PoolId}	aws:ResourceTag/ \${TagKey} (p. 1411)
SenderId	arn:\${Partition}:sms-voice:\${Region}: \${Account}:sender-id/\${SenderId}/ \${IsoCountryCode}	aws:ResourceTag/ \${TagKey} (p. 1411)

Condition keys for Amazon Pinpoint SMS Voice V2

Amazon Pinpoint SMS 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 [Available global condition 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 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 \(p. 1411\)](#)
- [Resource types defined by Amazon Polly \(p. 1412\)](#)
- [Condition keys for Amazon Polly \(p. 1413\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 permissions to delete the specified pronunciation lexicon stored in an AWS Region	Write	lexicon* (p. 1412)		
DescribeVoices	Grants permissions to describe the list of voices that are available for use when requesting speech synthesis	List			
GetLexicon	Grants permissions to retrieve the content of the specified pronunciation lexicon stored in an AWS Region	Read	lexicon* (p. 1412)		
GetSpeechSynthesisTask	Grants permissions to get information about specific speech synthesis task	Read			
ListLexicons	Grants permissions to list the pronunciation lexicons stored in an AWS Region	List			
ListSpeechSynthesisTasks	Grants permissions to list requested speech synthesis tasks	List			
PutLexicon	Grants permissions to store a pronunciation lexicon in an AWS Region	Write	lexicon* (p. 1412)		
StartSpeechSynthesis	Grants permissions to synthesize long inputs to the provided S3 location	Write	lexicon (p. 1412)		s3:PutObject
SynthesizeSpeech	Grants permissions to synthesize speech	Read	lexicon (p. 1412)		

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 \(p. 1411\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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 [Available keys for conditions](#).

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 \(p. 1413\)](#)
- [Resource types defined by AWS Price List \(p. 1414\)](#)
- [Condition keys for AWS Price List \(p. 1414\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeServices	Returns the service details for all (paginated) services (if <code>serviceCode</code> is not set) or service detail for a particular service (if given <code>serviceCode</code>).	Read			
GetAttributeValue	Returns all (paginated) possible values for a given attribute.	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetProducts	Returns all matching products with given search criteria.	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 [Available keys for conditions](#).

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 \(p. 1414\)](#)
- [Resource types defined by AWS Proton \(p. 1424\)](#)
- [Condition keys for AWS Proton \(p. 1425\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptEnvironmentConnection	Grants permission to reject a connection request from another environment account	Write	environment-account-connection* (p. 1425)		
CancelEnvironmentDeployment	Grants permission to cancel an environment deployment	Write	environment* (p. 1425)		proton:EnvironmentTemplate (p. 1426)
CancelServiceInstanceDeployment	Grants permission to cancel a service instance deployment	Write	service-instance* (p. 1425)		proton:ServiceTemplate (p. 1426)
CancelServicePipelineDeployment	Grants permission to cancel a service pipeline deployment	Write	service* (p. 1425)		proton:ServiceTemplate (p. 1426)
CreateEnvironment	Grants permission to create an environment	Write	environment* (p. 1425)	iam:PassRole	
				aws:TagKeys (p. 1425)	
CreateEnvironmentConnection	Grants permission to create an environment account connection	Write	aws:RequestTag/\${TagKey} (p. 1425)		aws:TagKeys (p. 1425)
CreateEnvironmentTemplate	Grants permission to create an environment template	Write	environment-template* (p. 1424)		
				aws:TagKeys (p. 1425)	
CreateEnvironmentTemplateMajor	Grants permission to create an environment template major version. DEPRECATED - use CreateEnvironmentTemplateVersion instead	Write	environment-template* (p. 1424)		
				aws:TagKeys (p. 1425)	
CreateEnvironmentTemplateMinor	Grants permission to create an environment template minor version. DEPRECATED - use CreateEnvironmentTemplateVersion instead	Write	environment-template* (p. 1424)		
				aws:TagKeys (p. 1425)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateEnvironmentTemplate	Grants permission to create an environment template version	Write	environment-template* (p. 1424)		
			aws:TagKeys (p. 1425)	aws:RequestTag/\${TagKey} (p. 1425)	
CreateRepository	Grants permission to create a repository	Write	repository* (p. 1425)		
			aws:TagKeys (p. 1425)	aws:RequestTag/\${TagKey} (p. 1425)	
CreateService	Grants permission to create a service	Write	service* (p. 1425)	codestar-connections:PassConnect	
			aws:TagKeys (p. 1425)	aws:RequestTag/\${TagKey} (p. 1425)	
			proton:ServiceTemplate (p. 1426)		
			aws:TagKeys (p. 1425)	aws:RequestTag/\${TagKey} (p. 1425)	
CreateServiceTemplate	Grants permission to create a service template	Write	service-template* (p. 1425)		
			aws:TagKeys (p. 1425)	aws:RequestTag/\${TagKey} (p. 1425)	
CreateServiceTemplateVersion	Grants permission to create a service template major version. DEPRECATED - use CreateServiceTemplateVersion instead	Write	service-template* (p. 1425)		
			aws:TagKeys (p. 1425)	aws:RequestTag/\${TagKey} (p. 1425)	
CreateServiceTemplateMinorVersion	Grants permission to create a service template minor version. DEPRECATED - use CreateServiceTemplateVersion instead	Write	service-template* (p. 1425)		
			aws:TagKeys (p. 1425)	aws:RequestTag/\${TagKey} (p. 1425)	
CreateServiceTemplateVersion	Grants permission to create a service template version	Write	service-template* (p. 1425)		
			aws:TagKeys (p. 1425)	aws:RequestTag/\${TagKey} (p. 1425)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTemplateSyncConfig	Grants permission to create a template sync config	Write			
DeleteAccountRole	Grants permission to delete account roles. DEPRECATED - use UpdateAccountSettings instead	Write			
DeleteEnvironment	Grants permission to delete an environment	Write	environment* (p. 1425)		
DeleteEnvironmentAccountConnection	Grants permission to delete an environment account connection		environment-account-connection* (p. 1425)		
DeleteEnvironmentTemplate	Grants permission to delete an environment template	Write	environment-template* (p. 1424)		
DeleteEnvironmentTemplateMajorVersion	Grants permission to delete an environment template major version. DEPRECATED - use DeleteEnvironmentTemplateVersion instead	Write	environment-template* (p. 1424)		
DeleteEnvironmentTemplateMinorVersion	Grants permission to delete an environment template minor version. DEPRECATED - use DeleteEnvironmentTemplateVersion instead	Write	environment-template* (p. 1424)		
DeleteEnvironmentTemplateVersion	Grants permission to delete an environment template version	Write	environment-template* (p. 1424)		
DeleteRepository	Grants permission to delete a repository	Write	repository* (p. 1425)		
DeleteService	Grants permission to delete a service	Write	service* (p. 1425)		
DeleteServiceTemplate	Grants permission to delete a service template		service-template* (p. 1425)		
DeleteServiceTemplateMajorVersion	Grants permission to delete a service template major version. DEPRECATED - use DeleteServiceTemplateVersion instead	Write	service-template* (p. 1425)		
DeleteServiceTemplateMinorVersion	Grants permission to delete a service template minor version. DEPRECATED - use DeleteServiceTemplateVersion instead	Write	service-template* (p. 1425)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteServiceTemplate	Grants permission to delete a service template version	Write	service-template* (p. 1425)		
DeleteTemplateSyncConfig	Grants permission to delete a template sync config	Write			
GetAccountRoles	Grants permission to get account roles. DEPRECATED - use GetAccountSettings instead	Read			
GetAccountSettings	Grants permission to describe the account settings	Read			
GetEnvironment	Grants permission to describe an environment	Read	environment* (p. 1425)		
GetEnvironmentAccountConnection	Grants permission to describe an environment account connection	Read	environment-account-connection* (p. 1425)		
GetEnvironmentTemplate	Grants permission to describe an environment template	Read	environment-template* (p. 1424)		
GetEnvironmentTemplateMajorVersion	Grants permission to get an environment template major version. DEPRECATED - use GetEnvironmentTemplateVersion instead	Read	environment-template* (p. 1424)		
GetEnvironmentTemplateMinorVersion	Grants permission to get an environment template minor version. DEPRECATED - use GetEnvironmentTemplateVersion instead	Read	environment-template* (p. 1424)		
GetEnvironmentTemplateVersion	Grants permission to describe an environment template version	Read	environment-template* (p. 1424)		
GetRepository	Grants permission to describe a repository	Read	repository* (p. 1425)		
GetRepositorySyncStatus	Grants permission to get the latest sync status for a repository	Read			
GetService	Grants permission to describe a service	Read	service* (p. 1425)		
GetServiceInstance	Grants permission to describe a service instance	Read	service-instance* (p. 1425)		
GetServiceTemplate	Grants permission to describe a service template	Read	service-template* (p. 1425)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetServiceTemplate	Grants permission to get a <code>serviceTemplate</code> major version. DEPRECATED - use <code>GetServiceTemplateVersion</code> instead	Read	<code>service-template*</code> (p. 1425)		
GetServiceTemplate	Grants permission to get a <code>serviceTemplate</code> minor version. DEPRECATED - use <code>GetServiceTemplateVersion</code> instead	Read	<code>service-template*</code> (p. 1425)		
GetServiceTemplate	Grants permission to describe a <code>serviceTemplate</code> version	Read	<code>service-template*</code> (p. 1425)		
GetTemplateSync	Grants permission to describe a <code>TemplateSyncConfig</code>	Read			
GetTemplateSync	Grants permission to describe the sync status of a template	Read			
ListEnvironmentAccounts	Grants permission to list <code>environmentAccount</code> connections	List	<code>environment-account-connection*</code> (p. 1425)		
ListEnvironmentOutputs	Grants permission to list <code>environment</code> outputs	List	<code>environment*</code> (p. 1425)		
ListEnvironmentProvisionedResources	Grants permission to list <code>environment</code> provisioned resources	List	<code>environment*</code> (p. 1425)		
ListEnvironmentTemplates	Grants permission to list <code>environmentTemplate</code> major versions. DEPRECATED - use <code>ListEnvironmentTemplateVersions</code> instead	List	<code>environment-template*</code> (p. 1424)		
ListEnvironmentTemplateMinorVersions	Grants permission to list an <code>environmentTemplate</code> minor versions. DEPRECATED - use <code>ListEnvironmentTemplateVersions</code> instead	List	<code>environment-template*</code> (p. 1424)		
ListEnvironmentTemplateVersions	Grants permission to list <code>environmentTemplate</code> versions	List	<code>environment-template*</code> (p. 1424)		
ListEnvironmentTemplates	Grants permission to list <code>environment</code> templates	List			
ListEnvironments	Grants permission to list environments	List			
ListRepositories	Grants permission to list repositories	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListRepositorySyncs	Grants permission to list repository sync definitions	List			
ListServiceInstances	Grants permission to list service instance outputs	List	service* (p. 1425)		
			service-instance* (p. 1425)		
ListServiceInstanceProvisionedResources	Grants permission to list service instance provisioned resources	List	service* (p. 1425)		
			service-instance* (p. 1425)		
ListServiceInstances	Grants permission to list service instances	List			
ListServicePipelineOutputs	Grants permission to list service pipeline outputs	List	service* (p. 1425)		
ListServicePipelineProvisionedResources	Grants permission to list service pipeline provisioned resources	List	service* (p. 1425)		
ListServiceTemplateMajorVersions	Grants permission to list service template major versions. DEPRECATED - use ListServiceTemplateVersions instead	List	service-template* (p. 1425)		
ListServiceTemplateMinorVersions	Grants permission to list service template minor versions. DEPRECATED - use ListServiceTemplateVersions instead	List	service-template* (p. 1425)		
ListServiceTemplateVersions	Grants permission to list service template versions	List	service-template* (p. 1425)		
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	environment (p. 1425)		
environment-template (p. 1424)					
environment-template-major-version (p. 1424)					
environment-template-minor-version (p. 1425)					

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			environment-template-version (p. 1424)		
			repository (p. 1425)		
			service (p. 1425)		
			service-instance (p. 1425)		
			service-template (p. 1425)		
			service-template-major-version (p. 1425)		
			service-template-minor-version (p. 1425)		
			service-template-version (p. 1425)		
NotifyResourceDeploymentOfResourceChange	Grants permission to notify AWS Proton of Resource deployment status changes	Write	environment (p. 1425)		
	service-instance (p. 1425)				
RejectEnvironmentConnectionRequest	Grants permission to reject an environment account connection request from another environment account	Write	environment-account-connection* (p. 1425)		
TagResource	Grants permission to add tags to a resource	Tagging	environment (p. 1425)		
	environment-template (p. 1424)				
	environment-template-major-version (p. 1424)				
	environment-template-minor-version (p. 1425)				
	environment-template-version (p. 1424)				

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			repository (p. 1425) service (p. 1425) service-instance (p. 1425) service-template (p. 1425)		
			service-template-major-version (p. 1425)		
			service-template-minor-version (p. 1425)		
			service-template-version (p. 1425)		
				aws:TagKeys (p. 1425) aws:RequestTag/\${TagKey} (p. 1425)	
UntagResource	Grants permission to remove tags from a resource	Tagging	environment (p. 1425)		
			environment-template (p. 1424)		
			environment-template-major-version (p. 1424)		
			environment-template-minor-version (p. 1425)		
			environment-template-version (p. 1424)		
			repository (p. 1425)		
			service (p. 1425)		
			service-instance (p. 1425)		

Service Authorization Reference
Service Authorization Reference
AWS Proton

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			service-template (p. 1425)		
			service-template-major-version (p. 1425)		
			service-template-minor-version (p. 1425)		
			service-template-version (p. 1425)		
				aws:TagKeys (p. 1425)	
UpdateAccountRole	Grants permission to update account roles. DEPRECATED - use UpdateAccountSettings instead	Write			iam:PassRole
UpdateAccountSettings	Grants permission to update the account settings	Write			iam:PassRole
UpdateEnvironment	Grants permission to update an environment	Write	environment* (p. 1425)	iam:PassRole	
				proton:EnvironmentTemplate (p. 1426)	
UpdateEnvironmentConnection	Grants permission to update an environment connection	Write	environment-account-connection* (p. 1425)		
UpdateEnvironmentTemplate	Grants permission to update an environment template	Write	environment-template* (p. 1424)		
UpdateEnvironmentTemplateVersion	Grants permission to update an environment template major version. DEPRECATED - use UpdateEnvironmentTemplateVersion instead	Write	environment-template* (p. 1424)		
UpdateEnvironmentTemplateVersion	Grants permission to update an environment template minor version. DEPRECATED - use UpdateEnvironmentTemplateVersion instead	Write	environment-template* (p. 1424)		
UpdateEnvironmentTemplateVersion	Grants permission to update an environment template version	Write	environment-template* (p. 1424)		
UpdateService	Grants permission to update a service	Write	service* (p. 1425)		
				proton:ServiceTemplate (p. 1426)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateServiceInstance	Grants permission to update a service instance	Write	service-instance* (p. 1425)		
				proton:ServiceTemplate (p. 1426)	
UpdateServicePipeline	Grants permission to update a service pipeline	Write	service* (p. 1425)		
				proton:ServiceTemplate (p. 1426)	
UpdateServiceTemplate	Grants permission to update a service template	Write	service-template* (p. 1425)		
UpdateServiceTemplateMajorVersion	Grants permission to update a service template major version. DEPRECATED - use UpdateServiceTemplateVersion instead	Write	service-template* (p. 1425)		
UpdateServiceTemplateMinorVersion	Grants permission to create a service template minor version. DEPRECATED - use UpdateServiceTemplateVersion instead	Write	service-template* (p. 1425)		
UpdateServiceTemplateVersion	Grants permission to update a service template version	Write	service-template* (p. 1425)		
UpdateTemplateSyncConfig	Grants permission to update a template sync config	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 \(p. 1414\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1425)
environment-template-version	arn:\${Partition}:proton:\${Region}: \${Account}:environment-template/ \${TemplateName}: \${MajorVersion}. \${MinorVersion}	aws:ResourceTag/ \${TagKey} (p. 1425)
environment-template-major-version	arn:\${Partition}:proton:\${Region}: \${Account}:environment-template/ \${TemplateName}: \${MajorVersionId}	aws:ResourceTag/ \${TagKey} (p. 1425)

Resource types	ARN	Condition keys
environment-template-minor-version	arn:\${Partition}:proton:\${Region}: \${Account}:environment-template/ \${TemplateName}: \${MajorVersionId}. \${MinorVersionId}	aws:ResourceTag/\${TagKey} (p. 1425)
service-template	arn:\${Partition}:proton:\${Region}: \${Account}:service-template/\${Name}	aws:ResourceTag/\${TagKey} (p. 1425)
service-template-version	arn:\${Partition}:proton:\${Region}: \${Account}:service-template/\${TemplateName}: \${MajorVersion}.\${MinorVersion}	aws:ResourceTag/\${TagKey} (p. 1425)
service-template-major-version	arn:\${Partition}:proton:\${Region}: \${Account}:service-template/\${TemplateName}: \${MajorVersionId}	aws:ResourceTag/\${TagKey} (p. 1425)
service-template-minor-version	arn:\${Partition}:proton:\${Region}: \${Account}:service-template/\${TemplateName}: \${MajorVersionId}. \${MinorVersionId}	aws:ResourceTag/\${TagKey} (p. 1425)
environment	arn:\${Partition}:proton:\${Region}: \${Account}:environment/\${Name}	aws:ResourceTag/\${TagKey} (p. 1425)
service	arn:\${Partition}:proton:\${Region}: \${Account}:service/\${Name}	aws:ResourceTag/\${TagKey} (p. 1425)
service-instance	arn:\${Partition}:proton:\${Region}: \${Account}:service/\${ServiceName}/service-instance/\${Name}	aws:ResourceTag/\${TagKey} (p. 1425)
environment-account-connection	arn:\${Partition}:proton:\${Region}: \${Account}:environment-account-connection/ \${Id}	aws:ResourceTag/\${TagKey} (p. 1425)
repository	arn:\${Partition}:proton:\${Region}: \${Account}:repository/\${Provider}: \${Name}	aws:ResourceTag/\${TagKey} (p. 1425)

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 [Available global condition 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

Condition keys	Description	Type
proton:EnvironmentTemplate	Filters actions based on specified environment template related to resource	String
proton:ServiceTemplate	Filters actions based on 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 \(p. 1426\)](#)
- [Resource types defined by AWS Purchase Orders Console \(p. 1427\)](#)
- [Condition keys for AWS Purchase Orders Console \(p. 1427\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyPurchaseOrderDetails [permission only]	Modify purchase orders and details	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ViewPurchaseOrders [permission only]	View purchase orders and details	Read			

Resource types defined by AWS Purchase Orders Console

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

Condition keys for AWS Purchase Orders Console

Purchase Orders 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 [Available keys for conditions](#).

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 \(p. 1427\)](#)
- [Resource types defined by Amazon QLDB \(p. 1430\)](#)
- [Condition keys for Amazon QLDB \(p. 1431\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources (“`*`”) in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1431)		
CreateLedger	Grants permission to create a ledger	Write	ledger* (p. 1431)		
				aws:RequestTag/\${TagKey} (p. 1431) aws:TagKeys (p. 1431)	
DeleteLedger	Grants permission to delete a ledger	Write	ledger* (p. 1431)		
DescribeJournalInformation	Grants permission to describe information about a journal kinesis stream	Read	stream* (p. 1431)		
DescribeJournalExportInformation	Grants permission to describe information about a journal export job	Read	ledger* (p. 1431)		
DescribeLedger	Grants permission to describe a ledger	Read	ledger* (p. 1431)		
ExecuteStatement	Grants permission to send commands to a ledger via the console	Write	ledger* (p. 1431)		
ExportJournalToS3	Grants permission to export journal contents to an Amazon S3 bucket	Write	ledger* (p. 1431)		
GetBlock	Grants permission to retrieve a block from a ledger for a given BlockAddress	Read	ledger* (p. 1431)		
GetDigest	Grants permission to retrieve a digest from a ledger for a given BlockAddress	Read	ledger* (p. 1431)		
GetRevision	Grants permission to retrieve a revision for a given document ID and a given BlockAddress	Read	ledger* (p. 1431)		
InsertSampleData	Grants permission to insert sample application data via the console	Write	ledger* (p. 1431)		
ListJournalKinesisStreams	Grants permission to list journal kinesis streams for a specified ledger	List	stream* (p. 1431)		

Service Authorization Reference
Service Authorization Reference
Amazon QLDB

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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* (p. 1431)		
ListLedgers	Grants permission to list existing ledgers	List			
ListTagsForResource	Grants permission to list tags for a resource	Read	catalog (p. 1431)		
			ledger (p. 1431)		
			stream (p. 1431)		
			table (p. 1431)		
PartiQLCreateIndex	Grants permission to create an index on a table	Write	table* (p. 1431)		
PartiQLCreateTable	Grants permission to create a table	Write	table* (p. 1431)		
			aws:RequestTag/ \${TagKey} (p. 1431)		
PartiQLDelete	Grants permission to delete documents from a table	Write	table* (p. 1431)		
			aws:TagKeys (p. 1431)		
PartiQLDropIndex	Grants permission to drop an index from a table	Write	table* (p. 1431)		
			qlldb:Purge (p. 1431)		
PartiQLDropTable	Grants permission to drop a table	Write	table* (p. 1431)		
			qlldb:Purge (p. 1431)		
PartiQLHistoryFunction	Grants permission to use the history function on a table	Read	table* (p. 1431)		
PartiQLInsert	Grants permission to insert documents into a table	Write	table* (p. 1431)		
PartiQLSelect	Grants permission to select documents from a table	Read	catalog (p. 1431)		
			table (p. 1431)		
PartiQLUndropTable	Grants permission to undrop a table	Write	table* (p. 1431)		
PartiQLUpdate	Grants permission to update existing documents in a table	Write	table* (p. 1431)		
SendCommand	Grants permission to send commands to a ledger	Write	ledger* (p. 1431)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ShowCatalog	Grants permission to view a ledger's catalog via the console	Write	ledger* (p. 1431)		
StreamJournalToJournal	Grants permission to stream Journal contents to a Kinesis Data Stream	Write	stream* (p. 1431) aws:RequestTag/ \${TagKey} (p. 1431) aws:TagKeys (p. 1431)		
TagResource	Grants permission to add one or more tags to a resource	Tagging	catalog (p. 1431) ledger (p. 1431) stream (p. 1431) table (p. 1431)		
aws:RequestTag/ \${TagKey} (p. 1431)	aws:TagKeys (p. 1431)				
catalog (p. 1431) ledger (p. 1431) stream (p. 1431) table (p. 1431)					
	aws:RequestTag/ \${TagKey} (p. 1431) aws:TagKeys (p. 1431)				
UpdateLedger	Grants permission to update properties on a ledger	Write	ledger* (p. 1431)		

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 \(p. 1427\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
ledger	arn:\${Partition}:qlldb:\${Region}: \${Account}:ledger/\${LedgerName}	aws:ResourceTag/\${TagKey} (p. 1431)
stream	arn:\${Partition}:qlldb:\${Region}: \${Account}:stream/\${LedgerName}/\${StreamId}	aws:ResourceTag/\${TagKey} (p. 1431)
table	arn:\${Partition}:qlldb:\${Region}: \${Account}:ledger/\${LedgerName}/table/\${TableId}	aws:ResourceTag/\${TagKey} (p. 1431)
catalog	arn:\${Partition}:qlldb:\${Region}: \${Account}:ledger/\${LedgerName}/information_schema/user_tables	aws:ResourceTag/\${TagKey} (p. 1431)

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 [Available global condition 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
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 \(p. 1432\)](#)
- [Resource types defined by Amazon QuickSight \(p. 1445\)](#)
- [Condition keys for Amazon QuickSight \(p. 1446\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AccountConfiguration [permission only]	Grants permission to enable setting default access to AWS resources	Write			
CancelIngestion	Grants permission to cancel a SPICE ingestions on a dataset	Write	ingestion* (p. 1445)		
				aws:RequestTag/\${TagKey} (p. 1446) aws:TagKeys (p. 1446)	
CreateAccountCustomization	Grants permission to create customization for QuickSight account or namespace	Write		aws:RequestTag/\${TagKey} (p. 1446) aws:TagKeys (p. 1446)	
CreateAdmin [permission only]	Grants permission to provision Amazon QuickSight administrators, authors, and readers	Write	user* (p. 1445)		
				aws:TagKeys (p. 1446) aws:RequestTag/\${TagKey} (p. 1446)	
CreateAnalysis	Grants permission to create an analysis from a template	Write	analysis* (p. 1445)		
				aws:RequestTag/\${TagKey} (p. 1446) aws:TagKeys (p. 1446)	

Service Authorization Reference
Service Authorization Reference
Amazon QuickSight

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCustomPermissions [permission only]	Grants permission to create a custom permissions resource for restricting user access	Permissions management		aws:RequestTag/\${TagKey} (p. 1446) aws:TagKeys (p. 1446)	
CreateDashboard	Grants permission to create a QuickSight Dashboard	Write	dashboard* (p. 1445)	aws:RequestTag/\${TagKey} (p. 1446) aws:TagKeys (p. 1446)	
CreateDataSet	Grants permission to create a dataset	Write	datasource* (p. 1445)	quicksight:PassDataSource	
CreateDataSource	Grants permission to create a data source	Write		aws:RequestTag/\${TagKey} (p. 1446) aws:TagKeys (p. 1446)	
CreateEmailCustomizationTemplate [permission only]	Grants permission to create a QuickSight template customization template	Write	emailCustomizationTemplate* (p. 1445)		
CreateFolder	Grants permission to create a QuickSight folder	Write	folder* (p. 1445)	aws:RequestTag/\${TagKey} (p. 1446) aws:TagKeys (p. 1446)	
CreateFolderMember	Grants permission to add a QuickSight Dashboard, Analysis or Dataset to a QuickSight Folder	Write	folder* (p. 1445) analysis (p. 1445) dashboard (p. 1445) dataset (p. 1445)		
CreateGroup	Grants permission to create a QuickSight group	Write	group* (p. 1445)	aws:TagKeys (p. 1446) aws:RequestTag/\${TagKey} (p. 1446)	
CreateGroupMember	Grants permission to add a QuickSight user to a QuickSight group	Write	group* (p. 1445)cksight:UserName (p. 1446)	aws:TagKeys (p. 1446) aws:RequestTag/\${TagKey} (p. 1446)	

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* (p. 1445)		
CreateIngestion	Grants permission to start a SPICE ingestion on a dataset	Write	ingestion* (p. 1445)		
				aws:RequestTag/\${TagKey} (p. 1446)	aws:TagKeys (p. 1446)
CreateNamespace	Grants permission to create an QuickSight namespace	Write	namespace* (p. 1445)	ds:CreateIdentityPoolDirectory	
				aws:RequestTag/\${TagKey} (p. 1446)	aws:TagKeys (p. 1446)
CreateReader [permission only]	Grants permission to provision Amazon QuickSight readers	Write	user* (p. 1445)		
				aws:TagKeys (p. 1446)	aws:RequestTag/\${TagKey} (p. 1446)
CreateTemplate	Grants permission to create a template	Write	template* (p. 1445)		
				aws:RequestTag/\${TagKey} (p. 1446)	aws:TagKeys (p. 1446)
CreateTemplateAlias	Grants permission to create a Template alias	Write	template* (p. 1445)		
				aws:RequestTag/\${TagKey} (p. 1446)	aws:TagKeys (p. 1446)
CreateTheme	Grants permission to create a theme	Write	theme* (p. 1445)		
				aws:RequestTag/\${TagKey} (p. 1446)	aws:TagKeys (p. 1446)
CreateThemeAlias	Grants permission to create an alias for a theme version	Write	theme* (p. 1445)		
				aws:RequestTag/\${TagKey} (p. 1446)	aws:TagKeys (p. 1446)

Service Authorization Reference
Service Authorization Reference
Amazon QuickSight

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateUser [permission only]	Grants permission to provision Amazon QuickSight authors and readers	Write	user* (p. 1445)		
	aws:TagKeys (p. 1446)		aws:RequestTag/\${TagKey} (p. 1446)		
CreateVPCConnection [permission only]	Grants permission to create a VPC connection	Write			
DeleteAccountCustomization	Grants permission to delete customization for QuickSight account or namespace	Write	customization* (p. 1445)		
DeleteAnalysis	Grants permission to delete an analysis	Write	analysis* (p. 1445)		
DeleteCustomPermissions [permission only]	Grants permission to delete a permissions resource	Permissions management			
DeleteDashboard	Grants permission to delete a QuickSight Dashboard	Write	dashboard* (p. 1445)		
DeleteDataSet	Grants permission to delete a dataset	Write	dataset* (p. 1445)		
	aws:RequestTag/\${TagKey} (p. 1446)		aws:TagKeys (p. 1446)		
DeleteDataSource	Grants permission to delete a data source	Write	datasource* (p. 1445)		
	aws:RequestTag/\${TagKey} (p. 1446)		aws:TagKeys (p. 1446)		
DeleteEmailCustomizationTemplate [permission only]	Grants permission to delete a QuickSight template customization template	Write	emailCustomizationTemplate* (p. 1445)		
DeleteFolder	Grants permission to delete a QuickSight Folder	Write	folder* (p. 1445)		
DeleteFolderMember	Grants permission to remove a QuickSight Dashboard, Analysis or Dataset from a QuickSight Folder	Write	folder* (p. 1445)		
analysis (p. 1445)					
dashboard (p. 1445)					
dataset (p. 1445)					

Service Authorization Reference
Service Authorization Reference
Amazon QuickSight

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteGroup	Grants permission to remove a user group from QuickSight	Write	group* (p. 1445)		
DeleteGroupMember	Grants permission to remove a user from a group so that he/she is no longer a member of the group	Write	group* (p. 1445) cksight:UserName (p. 1446)		
DeleteIAMPolicyAssignment	Grants permission to update an existing assignment	Write	assignment* (p. 1445)		
DeleteNamespace	Grants permission to delete a QuickSight namespace	Write	namespace* (p. 1445)		ds:DeleteDirectory
DeleteTemplate	Grants permission to delete a template	Write	template* (p. 1445)		
DeleteTemplateAlias	Grants permission to delete a template alias	Write	template* (p. 1445)		
DeleteTheme	Grants permission to delete a theme	Write	theme* (p. 1445)		
DeleteThemeAlias	Grants permission to delete the alias of a theme	Write	theme* (p. 1445)		
DeleteUser	Grants permission to delete a QuickSight user, given the user name	Write	user* (p. 1445)		
DeleteUserByPrincipal	Grants permission to delete a user identified by its principal ID	Write	user* (p. 1445)		
DeleteVPCConnection [permission only]	Grants permission to delete a VPC connection	Write			
DescribeAccountCustomization	Grants permission to describe customization for QuickSight account or namespace	Read	customization* (p. 1445)		
DescribeAccountSettings	Grants permission to describe the administrative account settings for QuickSight account	Read			
DescribeAnalysis	Grants permission to describe an analysis	Read	analysis* (p. 1445)		
DescribeAnalysisPermissions	Grants permission to describe permissions for an analysis	Read	analysis* (p. 1445)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeCustomPermissions [permission only]	Grants permission to describe a Custom permissions resource in a QuickSight account	Write			
DescribeDashboard	Grants permission to describe a QuickSight Dashboard	Read	dashboard* (p. 1445)		
DescribeDashboardPermissions	Grants permission to describe permissions for a QuickSight Dashboard	Read	dashboard* (p. 1445)		
DescribeDataSet	Grants permission to describe a dataset	Read	dataset* (p. 1445)		
			aws:RequestTag/ \${TagKey} (p. 1446)	aws:TagKeys (p. 1446)	
DescribeDataSetPermissions	Grants permission to describe the resource policy of a dataset	Permissions management	dataset* (p. 1445)		
				aws:RequestTag/ \${TagKey} (p. 1446)	aws:TagKeys (p. 1446)
DescribeDataSource	Grants permission to describe a data source	Read	datasource* (p. 1445)		
	aws:RequestTag/ \${TagKey} (p. 1446)		aws:TagKeys (p. 1446)		
DescribeDataSourcePermissions	Grants permission to describe the Resource policy of a data source	Permissions management	datasource* (p. 1445)		
				aws:RequestTag/ \${TagKey} (p. 1446)	aws:TagKeys (p. 1446)
DescribeEmailCustomizationTemplate [permission only]	Grants permission to describe a QuickSight Email customization template	Read	emailCustomizationTemplate* (p. 1445)		
DescribeFolder	Grants permission to describe a QuickSight Folder	Read	folder* (p. 1445)		
DescribeFolderPermissions	Grants permission to describe permissions for a QuickSight Folder	Read	folder* (p. 1445)		
DescribeFolderResolvedPermissions	Grants permission to describe resolved permissions for a QuickSight Folder	Read	folder* (p. 1445)		

Service Authorization Reference
Service Authorization Reference
Amazon QuickSight

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeGroup	Grants permission to describe a QuickSight group	Read	group* (p. 1445)		
DescribeGroupMember	Grants permission to describe a QuickSight group member	Read	group* (p. 1445) QuickSight:UserName (p. 1446)		
DescribeIAMPolicyAssignment	Grants permission to describe an existing assignment	Read	assignment* (p. 1445)		
DescribeIngestion	Grants permission to describe a SPICE ingestion on a dataset	Read	ingestion* (p. 1445)		
					aws:RequestTag/\${TagKey} (p. 1446)
DescribeIPRestriction	Grants permission to describe the IP restrictions for QuickSight account	Read			
DescribeNamespace	Grants permission to describe a QuickSight namespace	Read	namespace* (p. 1445)		
DescribeTemplate	Grants permission to describe a template	Read	template* (p. 1445)		
DescribeTemplateAlias	Grants permission to describe a template alias	Read	template* (p. 1445)		
DescribeTemplatePermissions	Grants permission to describe permissions for a template	Read	template* (p. 1445)		
DescribeTheme	Grants permission to describe a theme	Read	theme* (p. 1445)		
DescribeThemeAlias	Grants permission to describe a theme alias	Read	theme* (p. 1445)		
DescribeThemePermissions	Grants permission to describe permissions for a theme	Read	theme* (p. 1445)		
DescribeUser	Grants permission to describe a QuickSight user given the user name	Read	user* (p. 1445)		
GenerateEmbedURLRequest	Grants permission to generate a URL used to embed a QuickSight Dashboard for a user not registered with QuickSight	Write	dashboard* (p. 1445)		
			namespace* (p. 1445)		
			aws:TagKeys (p. 1446)		aws:RequestTag/\${TagKey} (p. 1446)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GenerateEmbedURL [used to embed a QuickSight Dashboard for a user registered with QuickSight]	Grants permission to generate a URL used to embed a QuickSight Dashboard for a user registered with QuickSight	Write	user* (p. 1445)		
GetAnonymousUserAuthCode [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* (p. 1445)		
GetDashboardEmbedURL	Grants permission to get a URL used to embed a QuickSight Dashboard	Read	dashboard* (p. 1445)		
GetGroupMapping [permission only]	Grants permission to use Amazon QuickSight, in Enterprise edition, to identify and display the Microsoft Active Directory (Microsoft Active Directory) directory groups that are mapped to roles in Amazon QuickSight	Read			
GetSessionEmbedURL	Grants permission to get a URL to embed QuickSight console experience	Read			
ListAnalyses	Grants permission to list all analyses in an account	List	analysis* (p. 1445)		
ListCustomPermissions [permission only]	Grants permission to list custom permissions resources in QuickSight account	Write			
ListDashboardVersions	Grants permission to list all versions of a QuickSight Dashboard	List	dashboard* (p. 1445)		
ListDashboards	Grants permission to list all Dashboards in a QuickSight Account	List	dashboard* (p. 1445)		
ListDataSets	Grants permission to list all datasets	List		aws:RequestTag/\${TagKey} (p. 1446)	aws:TagKeys (p. 1446)

Service Authorization Reference
Service Authorization Reference
Amazon QuickSight

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDataSources	Grants permission to list all data sources	List		aws:RequestTag/ \${TagKey} (p. 1446) aws:TagKeys (p. 1446)	
ListFolderMembers	Grants permission to list all members in a folder	Read	folder* (p. 1445)		
ListFolders	Grants permission to list all Folders in a QuickSight Account	List	folder* (p. 1445)		
ListGroupMembers	Grants permission to list member users in a group	List	group* (p. 1445)		
ListGroups	Grants permission to list all user groups in QuickSight	List	group* (p. 1445)		
ListIAMPolicyAssignments	Grants permission to list all assignments in the current Amazon QuickSight account	List	assignment* (p. 1445)		
ListIAMPolicyAssignmentForUser	Grants permission to list all assignments assigned to a user and the groups it belongs	List	assignment* (p. 1445)		
ListIngestions	Grants permission to list all SPICE ingestions on a dataset	List		aws:RequestTag/ \${TagKey} (p. 1446) aws:TagKeys (p. 1446)	
ListNamespaces	Grants permission to lists all namespaces in a QuickSight account	List			
ListTagsForResource	Grants permission to list tags of a QuickSight resource	Read	customization (p. 1445)		
			dashboard (p. 1445)		
			folder (p. 1445)		
			template (p. 1445)		
			theme (p. 1445)		
ListTemplateAliases	Grants permission to list all aliases for a template	List	template* (p. 1445)		
ListTemplateVersions	Grants permission to list all versions of a template	List	template* (p. 1445)		
ListTemplates	Grants permission to list all templates in a QuickSight account	List	template* (p. 1445)		
ListThemeAliases	Grants permission to list all aliases of a theme	List	theme* (p. 1445)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListThemeVersion	Grants permission to list all versions of a theme	List	theme* (p. 1445)		
ListThemes	Grants permission to list all themes in an account	List	theme* (p. 1445)		
ListUserGroups	Grants permission to list groups that a given user is a member of	List	user* (p. 1445)		
ListUsers	Grants permission to list all of the QuickSight users belonging to this account	List	user* (p. 1445)		
PassDataSet [permission only]	Grants permission to use a dataset for a template	Read	dataset* (p. 1445)		
				aws:RequestTag/\${TagKey} (p. 1446) aws:TagKeys (p. 1446)	
PassDataSource [permission only]	Grants permission to use a data source for a data set	Read	datasource* (p. 1445)		
				aws:RequestTag/\${TagKey} (p. 1446) aws:TagKeys (p. 1446)	
RegisterUser	Grants permission to create a QuickSight user, whose identity is associated with the IAM identity/role specified in the request	Write	user* (p. 1445) quicksight:iamArn (p. 1446) quicksight:SessionName (p. 1446)		
RestoreAnalysis	Grants permission to restore a deleted analysis	Write	analysis* (p. 1445)		
ScopeDownPolicy [permission only]	Grants permission to manage scoping policies for permissions to AWS resources	Write			
SearchAnalyses	Grants permission to search for a sub-set of analyses	List	analysis* (p. 1445)		
SearchDashboard	Grants permission to search for a sub-set of QuickSight Dashboards	List	dashboard* (p. 1445)		
SearchDirectoryGroup [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			

Service Authorization Reference
Service Authorization Reference
Amazon QuickSight

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SearchFolders	Grants permission to search for a sub-set of QuickSight Folders	Read	folder* (p. 1445)		
SearchGroups	Grants permission to search for a sub-set of QuickSight groups	List	group* (p. 1445)		
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			
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 (p. 1446) quicksight:DirectoryType (p. 1446)	
TagResource	Grants permission to add tags to a QuickSight resource	Tagging	customization (p. 1445) dashboard (p. 1445) folder (p. 1445) template (p. 1445) theme (p. 1445)		
			aws:TagKeys (p. 1446)	aws:RequestTag/ \${TagKey} (p. 1446)	
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	customization (p. 1445) dashboard (p. 1445) folder (p. 1445) template (p. 1445) theme (p. 1445)		
				aws:TagKeys (p. 1446)	

Service Authorization Reference
Service Authorization Reference
Amazon QuickSight

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAccountCustomization	Grants permission to update customization for QuickSight account or namespace	Write	customization* (p. 1445)		
UpdateAccountSettings	Grants permission to update the administrative account settings for QuickSight account	Write			
UpdateAnalysis	Grants permission to update an analysis	Write	analysis* (p. 1445)		
UpdateAnalysisPermissions	Grants permission to update permissions for an analysis	Permissions management	analysis* (p. 1445)		
UpdateCustomPermissions [permission only]	Grants permission to update a permissions resource	Permissions management			
UpdateDashboard	Grants permission to update a QuickSight Dashboard	Write	dashboard* (p. 1445)		
UpdateDashboardPermissions	Grants permission to update permissions for a QuickSight Dashboard	Permissions management	dashboard* (p. 1445)		
UpdateDashboardPublishedVersion	Grants permission to update a QuickSight Dashboard's Published Version	Write	dashboard* (p. 1445)		
UpdateDataSet	Grants permission to update a dataset	Write	dataset* (p. 1445)		quicksight:PassDataSource
			datasource (p. 1445)		
				aws:RequestTag/ \${TagKey} (p. 1446)	aws:TagKeys (p. 1446)
UpdateDataSetPermissions	Grants permission to update the resources policy of a dataset	Permissions management	dataset* (p. 1445)		
				aws:RequestTag/ \${TagKey} (p. 1446)	
				aws:TagKeys (p. 1446)	
UpdateDataSource	Grants permission to update a data source	Write	datasource* (p. 1445)		
				aws:RequestTag/ \${TagKey} (p. 1446)	
				aws:TagKeys (p. 1446)	
UpdateDataSourcePermissions	Grants permission to update the resources policy of a data source	Permissions management	datasource* (p. 1445)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 1446) aws:TagKeys (p. 1446)	
UpdateEmailCustomizationTemplate [permission only]	Grants permission to update a QuickSight Template customization template	Write	emailCustomizationTemplate* (p. 1445)		
UpdateFolder	Grants permission to update a QuickSight Folder	Write	folder* (p. 1445)		
UpdateFolderPermissions	Grants permission to update permissions for a QuickSight Folder	Permissions management	folder* (p. 1445)		
UpdateGroup	Grants permission to change group description	Write	group* (p. 1445)		
UpdateIAMPolicyAssignment	Grants permission to update an existing assignment	Write	assignment* (p. 1445)		
UpdateIpRestriction	Grants permission to update the IP restrictions for QuickSight account	Write			
UpdatePublicSharing	Grants permission to enable public sharing on an account	Write			
UpdateTemplate	Grants permission to update a template	Write	template* (p. 1445)		
UpdateTemplateAlias	Grants permission to update a template alias	Write	template* (p. 1445)		
UpdateTemplatePermissions	Grants permission to update permissions for a template	Permissions management	template* (p. 1445)		
UpdateTheme	Grants permission to update a theme	Write	theme* (p. 1445)		
UpdateThemeAlias	Grants permission to update the alias of a theme	Write	theme* (p. 1445)		
UpdateThemePermissions	Grants permission to update permissions for a theme	Permissions management	theme* (p. 1445)		
UpdateUser	Grants permission to update an Amazon QuickSight user	Write	user* (p. 1445)		

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 \(p. 1432\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
user	<code>arn:\${Partition}:quicksight:\${Region}: \${Account}:user/\${ResourceId}</code>	
group	<code>arn:\${Partition}:quicksight:\${Region}: \${Account}:group/\${ResourceId}</code>	
analysis	<code>arn:\${Partition}:quicksight:\${Region}: \${Account}:analysis/\${ResourceId}</code>	aws:ResourceTag/\${TagKey} (p. 1446)
dashboard	<code>arn:\${Partition}:quicksight:\${Region}: \${Account}:dashboard/\${ResourceId}</code>	aws:ResourceTag/\${TagKey} (p. 1446)
template	<code>arn:\${Partition}:quicksight:\${Region}: \${Account}:template/\${ResourceId}</code>	aws:ResourceTag/\${TagKey} (p. 1446)
datasource	<code>arn:\${Partition}:quicksight:\${Region}: \${Account}:datasource/\${ResourceId}</code>	aws:ResourceTag/\${TagKey} (p. 1446)
dataset	<code>arn:\${Partition}:quicksight:\${Region}: \${Account}:dataset/\${ResourceId}</code>	aws:ResourceTag/\${TagKey} (p. 1446)
ingestion	<code>arn:\${Partition}:quicksight:\${Region}: \${Account}:dataset/\${DatasetId}/ingestion/ \${ResourceId}</code>	aws:ResourceTag/\${TagKey} (p. 1446)
theme	<code>arn:\${Partition}:quicksight:\${Region}: \${Account}:theme/\${ResourceId}</code>	aws:ResourceTag/\${TagKey} (p. 1446)
assignment	<code>arn:\${Partition}:quicksight:: \${Account}:assignment/\${ResourceId}</code>	
customization	<code>arn:\${Partition}:quicksight:\${Region}: \${Account}:customization/\${ResourceId}</code>	aws:ResourceTag/\${TagKey} (p. 1446)
namespace	<code>arn:\${Partition}:quicksight:\${Region}: \${Account}:namespace/\${ResourceId}</code>	
folder	<code>arn:\${Partition}:quicksight:\${Region}: \${Account}:folder/\${ResourceId}</code>	aws:ResourceTag/\${TagKey} (p. 1446)
emailCustomizationTemplate	<code>arn:\${Partition}:quicksight:\${Region}: \${Account}:email-customization-template/ \${ResourceId}</code>	

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters access by tag key-value pairs in the request	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters access by tag key-value pairs attached to the resource	String
<code>aws:TagKeys</code>	Filters access by tag keys	ArrayOfString
<code>quicksight:DirectoryType</code>	Filters access by the user management options	String
<code>quicksight:Edition</code>	Filters access by the edition of QuickSight	String
<code>quicksight:IamArn</code>	Filters access by IAM user or role ARN	String
<code>quicksight:SessionName</code>	Filters access by session name	String
<code>quicksight:UserName</code>	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 \(p. 1446\)](#)
- [Resource types defined by Amazon RDS \(p. 1466\)](#)
- [Condition keys for Amazon RDS \(p. 1468\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1466)		iam:PassRole
AddRoleToDBInstance	Grants permission to associate an AWS Identity and Access Management (IAM) role with a DB instance	Write	db* (p. 1466)		iam:PassRole
AddSourceIdentifier	Grants permission to add a source identifier to an existing RDS event notification subscription	Write	es* (p. 1467)		
AddTagsToResource	Grants permission to add metadata tags to an Amazon RDS resource	Tagging	cev (p. 1468)		
			cluster (p. 1466)		
			cluster-endpoint (p. 1466)		
			cluster-pg (p. 1466)		
			cluster-snapshot (p. 1466)		
			db (p. 1466)		
			es (p. 1467)		
			og (p. 1467)		
			pg (p. 1467)		
			proxy (p. 1467)		
			proxy-endpoint (p. 1467)		
			ri (p. 1467)		

Service Authorization Reference
Service Authorization Reference
Amazon RDS

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			secgrp (p. 1467) snapshot (p. 1467) subgrp (p. 1468) target-group (p. 1468)		
				aws:RequestTag/\${TagKey} (p. 1468) aws:TagKeys (p. 1468) rds:req-tag/\${TagKey} (p. 1469)	
ApplyPendingMaintenanceAction	Grants permission to apply a pending maintenance action to a resource	Write	cluster (p. 1466) db (p. 1466)		
AuthorizeDBSecurityGroupIngress	Grants permission to enable access to a DB security group using one of two forms of authorization	Permissions management	secgrp* (p. 1467)		
BacktrackDBCluster	Grants permission to backtrack a DB cluster to a specific time, without creating a new DB cluster	Write	cluster* (p. 1466)		
CancelExportTask	Grants permission to cancel an export task in progress	Write			
CopyDBClusterParameterGroup	Grants permission to copy the specified DB cluster parameter group	Write	cluster-pg* (p. 1466)		rds:AddTagsToResource
				aws:RequestTag/\${TagKey} (p. 1468) aws:TagKeys (p. 1468)	
CopyDBClusterSnapshot	Grants permission to create a snapshot of a DB cluster	Write	cluster-snapshot* (p. 1466)		rds:AddTagsToResource
				aws:RequestTag/\${TagKey} (p. 1468) aws:TagKeys (p. 1468)	
CopyDBParameterGroup	Grants permission to copy the specified DB parameter group	Write	pg* (p. 1467)		rds:AddTagsToResource

Service Authorization Reference
Service Authorization Reference
Amazon RDS

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 1468) aws:TagKeys (p. 1468)	
CopyDBSnapshot	Grants permission to copy the specified DB snapshot	Write	snapshot* (p. 1467)	rds:AddTagsToResource	
				aws:RequestTag/ \${TagKey} (p. 1468) aws:TagKeys (p. 1468)	
CopyOptionGroup	Grants permission to copy the specified option group	Write	og* (p. 1467)	rds:AddTagsToResource	
				aws:RequestTag/ \${TagKey} (p. 1468) aws:TagKeys (p. 1468)	
CreateCustomDBEngineVersion	Grants permission to create a custom engine version	Write	cev* (p. 1468)	iam>CreateServiceLinkedRole mediaimport>CreateData rds:AddTagsToResource	
				aws:RequestTag/ \${TagKey} (p. 1468) aws:TagKeys (p. 1468)	
CreateDBCluster	Grants permission to create a new Amazon Aurora DB cluster	Write	cluster* (p. 1466)	iam:PassRole rds:AddTagsToResource rds>CreateDBInstance	
			cluster- pg* (p. 1466)		
			og* (p. 1467)		
			subgrp* (p. 1468)		
			db (p. 1466)		
			global- cluster (p. 1467)		

Service Authorization Reference
Service Authorization Reference
Amazon RDS

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/\${TagKey} (p. 1468) aws:TagKeys (p. 1468) rds:req-tag/\${TagKey} (p. 1469) rds:DatabaseEngine (p. 1468) rds:DatabaseName (p. 1468) rds:StorageEncrypted (p. 1469) rds:DatabaseClass (p. 1468) rds:StorageSize (p. 1469) rds:Piops (p. 1468)	
CreateDBClusterEndpoint	Grants permission to create a new custom endpoint and associates it with an Amazon Aurora DB cluster	Write	cluster* (p. 1466)		rds:AddTagsToResource
			cluster-endpoint* (p. 1466)		
				rds:EndpointType (p. 1468) aws:RequestTag/\${TagKey} (p. 1468) aws:TagKeys (p. 1468)	
CreateDBClusterParameterGroup	Grants permission to create a new DB cluster parameter group	Write	cluster-pg* (p. 1466)		rds:AddTagsToResource
				aws:RequestTag/\${TagKey} (p. 1468) aws:TagKeys (p. 1468) rds:req-tag/\${TagKey} (p. 1469)	
CreateDBClusterSnapshot	Grants permission to create a snapshot of a DB cluster	Write	cluster* (p. 1466)		rds:AddTagsToResource
			cluster-snapshot* (p. 1466)		

Service Authorization Reference
Service Authorization Reference
Amazon RDS

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 1468) aws:TagKeys (p. 1468) rds:req- tag/ \${TagKey} (p. 1469)	
CreateDBInstance	Grants permission to create a new DB instance	Write	db* (p. 1466) cluster (p. 1466) og (p. 1467) pg (p. 1467) secgrp (p. 1467) subgrp (p. 1468)	rds:BackupTarget (p. 1468) aws:RequestTag/ \${TagKey} (p. 1468) aws:TagKeys (p. 1468) rds:req- tag/ \${TagKey} (p. 1469)	iam:PassRole rds:AddTagsToResource
CreateDBInstance	Grants permission to create a DB instance that acts as a Read Replica of a source DB instance	Write	db* (p. 1466) og* (p. 1467) subgrp* (p. 1468)	aws:RequestTag/ \${TagKey} (p. 1468) aws:TagKeys (p. 1468) rds:req- tag/ \${TagKey} (p. 1469)	iam:PassRole rds:AddTagsToResource
CreateDBParameterGroup	Grants permission to create a new DB parameter group	Write	pg* (p. 1467)		rds:AddTagsToResource

Service Authorization Reference
Service Authorization Reference
Amazon RDS

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 1468) aws:TagKeys (p. 1468) rds:req- tag/ \${TagKey} (p. 1469)	
CreateDBProxy	Grants permission to create a database proxy	Write		aws:RequestTag/ \${TagKey} (p. 1468) aws:TagKeys (p. 1468)	
CreateDBProxyEndpoint	Grants permission to create a database proxy endpoint	Write	proxy* (p. 1467) proxy- endpoint* (p. 1467)		
CreateDBSecurityGroup	Grants permission to create a new DB security group. DB security groups control access to a DB instance	Write	secgrp* (p. 1467)	rds:AddTagsToResource	
CreateDBSnapshot	Grants permission to create a DBSnapshot	Write	db* (p. 1466) snapshot* (p. 1467)	rds:AddTagsToResource	
CreateDBSubnetGroup	Grants permission to create a new DB subnet group	Write	subgrp* (p. 1468)	rds:AddTagsToResource	

Service Authorization Reference
Service Authorization Reference
Amazon RDS

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 1468) aws:TagKeys (p. 1468) rds:req- tag/ \${TagKey} (p. 1469)	
CreateEventSubscription	Grants permission to create an RDS event notification subscription	Write	es* (p. 1467)		rds:AddTagsToResource
				aws:RequestTag/ \${TagKey} (p. 1468) aws:TagKeys (p. 1468) rds:req- tag/ \${TagKey} (p. 1469)	
CreateGlobalCluster	Grants permission to create an Aurora global database spread across multiple regions	Write	cluster* (p. 1466) global- cluster* (p. 1467)		
CreateOptionGroup	Grants permission to create a new option group	Write	og* (p. 1467)		rds:AddTagsToResource
				aws:RequestTag/ \${TagKey} (p. 1468) aws:TagKeys (p. 1468) rds:req- tag/ \${TagKey} (p. 1469)	
CrossRegionCopy	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			
DeleteCustomDBEngineVersion	Grants permission to delete an existing custom engine version	Write	cev* (p. 1468)		
DeleteDBCluster	Grants permission to delete a previously provisioned DB cluster	Write	cluster* (p. 1466) cluster- snapshot* (p. 1466)		rds:DeleteDBInstance
DeleteDBClusterEndpoint	Grants permission to delete a custom endpoint and removes it from an Amazon Aurora DB cluster	Write	cluster- endpoint* (p. 1466)		

Service Authorization Reference
Service Authorization Reference
Amazon RDS

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteDBClusterParameterGroup	Grants permission to delete a specified DB cluster parameter group	Write	cluster- pg* (p. 1466)		
DeleteDBClusterSnapshot	Grants permission to delete a DB cluster snapshot	Write	cluster- snapshot* (p. 1466)		
DeleteDBInstance	Grants permission to delete a previously provisioned DB instance	Write	db* (p. 1466)		
DeleteDBInstanceAutomatedBackups	Grants permission to delete automated backups based on the source instance's DbiResourceId value or the restorable instance's resource ID	Write			
DeleteDBParameterGroup	Grants permission to delete a specified DBParameterGroup	Write	pg* (p. 1467)		
DeleteDBProxy	Grants permission to delete a database proxy	Write	proxy* (p. 1467)		
DeleteDBProxyEndpoint	Grants permission to delete a database proxy endpoint	Write	proxy- endpoint* (p. 1467)		
DeleteDBSecurityGroup	Grants permission to delete a DB security group	Write	secgrp* (p. 1467)		
DeleteDBSnapshot	Grants permission to delete a DBSnapshot	Write	snapshot* (p. 1467)		
DeleteDBSubnetGroup	Grants permission to delete a DBSubnet group	Write	subgrp* (p. 1468)		
DeleteEventSubscription	Grants permission to delete an RDS event notification subscription	Write	es* (p. 1467)		
DeleteGlobalCluster	Grants permission to delete a global database cluster	Write	global- cluster* (p. 1467)		
DeleteOptionGroup	Grants permission to delete an existing option group	Write	og* (p. 1467)		
DeregisterDBProxyTargets	Grants permission to remove targets from a database proxy target group	Write	cluster* (p. 1466)		
db* (p. 1466)					
proxy* (p. 1467)					
target- group* (p. 1468)					

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeAccountAttributes	Grants permission to list all of the attributes for a customer account	List			
DescribeCertificates	Grants permission to list the set of CA certificates provided by Amazon RDS for this AWS account	List			
DescribeDBClusterInformation	Grants permission to return information about backtracks for a DB cluster	List	cluster* (p. 1466)		
DescribeDBClusterInformation	Grants permission to return information about endpoints for an Amazon Aurora DB cluster	List	cluster-endpoint* (p. 1466)		
			cluster (p. 1466)		
DescribeDBClusterParameterGroups	Grants permission to return a list of DB cluster ParameterGroup descriptions	List	cluster-pg* (p. 1466)		
DescribeDBClusterParameters	Grants permission to return the detailed parameter list for a particular DB cluster parameter group	List	cluster-pg* (p. 1466)		
DescribeDBClusterSnapshotAttributes	Grants permission to return a list of DB cluster snapshot attribute names and values for a manual DB cluster snapshot	List	cluster-snapshot* (p. 1466)		
DescribeDBClusterSnapshots	Grants permission to return information about DB cluster snapshots	List	cluster-snapshot* (p. 1466)		
DescribeDBClusters	Grants permission to return information about provisioned Aurora DB clusters	List	cluster* (p. 1466)		
DescribeDBEngines	Grants permission to return a list of the available DB engines	List			
DescribeDBInstances	Grants permission to return a list of Automated Backups for both current and deleted instances	List	db (p. 1466)		
DescribeDBInstances	Grants permission to return information about provisioned RDS instances	List	db* (p. 1466)		
DescribeDBLogFileList	Grants permission to return a list of DB log files for the DB instance	List	db* (p. 1466)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDBParameterGroups	Grants permission to return a list of DBParameterGroup descriptions	List	pg* (p. 1467)		
DescribeDBParameters	Grants permission to return the detailed parameter list for a particular DB parameter group	List	pg* (p. 1467)		
DescribeDBProxies	Grants permission to view proxies	List	proxy* (p. 1467)		
DescribeDBProxyEndpoints	Grants permission to view proxy endpoints	List	proxy* (p. 1467)		
DescribeDBProxyTargetGroups	Grants permission to view database proxy target group details		proxy* (p. 1467)		
DescribeDBProxyTargets	Grants permission to view database proxy target details	List	cluster* (p. 1466)		
			db* (p. 1466)		
			proxy* (p. 1467)		
			target-group* (p. 1468)		
DescribeDBSecurityGroups	Grants permission to return a list of DBSecurityGroup descriptions	List	secgrp* (p. 1467)		
DescribeDBSnapshots	Grants permission to return a list of DBsnapshot attribute names and values for a manual DB snapshot	List	snapshot* (p. 1467)		
DescribeDBSnapshotInformation	Grants permission to return information about DB snapshots	List	snapshot* (p. 1467)		
			db (p. 1466)		
DescribeDBSubnets	Grants permission to return a list of DBsubnetGroup descriptions	List	subgrp* (p. 1468)		
DescribeEngineDefaultParameters	Grants permission to return the default engine and system parameter information for the cluster database engine	List			
DescribeEngineDefaultParametersForEngine	Grants permission to return the default engine and system parameter information for the specified database engine	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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* (p. 1467)		
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			
DescribeGlobalClusters	Grants permission to return information about Aurora global database clusters	List	global-cluster* (p. 1467)		
DescribeOptionGroups	Grants permission to describe all available options	List	og* (p. 1467)		
DescribeOptionGroupDetails	Grants permission to describe the available option groups	List	og* (p. 1467)		
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 pending maintenance actions (for example, DB instances) that have at least one pending maintenance action	List	cluster (p. 1466)		
			db (p. 1466)		
DescribeRecommendations [permission only]	Grants permission to return information about recommendation groups	Read			
DescribeRecommendationDetails [permission only]	Grants permission to return information about recommendations	Read			
DescribeReservedInstances	Grants permission to return information about reserved DB instances for this account, or about a specified reserved DB instance	List	ri* (p. 1467)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeReservedDBInstancesOfferings	Grants permission to list available reserved DB instance offerings	List			
DescribeSourceRegions	Grants permission to return a list of the source AWS Regions where the current AWS Region can create a Read Replica or copy a DB snapshot from	List			
DescribeValidDBModifications	Grants permission to list available modifications you can make to your DB instance	List	db* (p. 1466)		
DownloadComprehensiveLog	Grants permission to download specified log file	Read	db* (p. 1466)		
DownloadDBLog	Grants permission to download a portion of the specified log file, up to 1 MB in size	Read	db* (p. 1466)		
FailoverDBCluster	Grants permission to force a failover for a DB cluster	Write	cluster* (p. 1466)		
FailoverGlobalCluster	Grants permission to failover a global cluster	Write	cluster* (p. 1466)	global-cluster* (p. 1467)	
ListTagsForResource	Grants permission to list all tags on an Amazon RDS resource	Read	cev (p. 1468)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			secgrp (p. 1467)		
			snapshot (p. 1467)		
			subgrp (p. 1468)		
			target-group (p. 1468)		
ModifyCertificate	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 capacity for an Amazon Aurora Serverless DB cluster	Write	cluster* (p. 1466)		
ModifyCustomDBEngineVersion	Grants permission to modify an existing custom engine version	Write	cev* (p. 1468)		
ModifyDBCluster	Grants permission to modify a setting for an Amazon Aurora DB cluster	Write	cluster* (p. 1466)		iam:PassRole rds:ModifyDBInstance
cluster-pg* (p. 1466)					
og* (p. 1467)					
	rds:DatabaseClass (p. 1468)				
ModifyDBClusterEndpoint	Grants permission to modify the properties of an endpoint in an Amazon Aurora DB cluster	Write	cluster-endpoint* (p. 1466)		
ModifyDBClusterParameterGroup	Grants permission to modify the parameters of a DB cluster parameter group	Write	cluster-pg* (p. 1466)		
ModifyDBClusterSnapshotAttributeAndValues	Grants permission to add an attribute and values to, or removes an attribute and values from, a manual DB cluster snapshot	Write	cluster-snapshot* (p. 1466)		
ModifyDBInstance	Grants permission to modify settings for a DB instance	Write	db* (p. 1466)		iam:PassRole
og* (p. 1467)					
pg* (p. 1467)					

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			secgrp* (p. 1467)		
ModifyDBParameterGroup	Grants permission to modify the parameters of a DB parameter group	Write	pg* (p. 1467)		
ModifyDBProxy	Grants permission to modify database proxy	Write	proxy* (p. 1467)		iam:PassRole
ModifyDBProxyEndpoint	Grants permission to modify database proxy endpoint	Write	proxy-endpoint* (p. 1467)		
ModifyDBProxyTargetGroup	Grants permission to modify target group for a database proxy	Write	target-group* (p. 1468)		
ModifyDBSnapshot	Grants permission to update a manual DB snapshot, which can be encrypted or not encrypted, with a new engine version	Write	snapshot* (p. 1467)		
ModifyDBSnapshotAttribute	Grants permission to add an attribute and values to, or removes an attribute and values from, a manual DB snapshot	Write	snapshot* (p. 1467)		
ModifyDBSubnetGroup	Grants permission to modify an existing DB subnet group	Write	subgrp* (p. 1468)		
ModifyEventSubscription	Grants permission to modify an existing RDS event notification subscription	Write	es* (p. 1467)		
ModifyGlobalClusterSetting	Grants permission to modify a setting for an Amazon Aurora global cluster	Write	global-cluster* (p. 1467)		
ModifyOptionGroup	Grants permission to modify an existing option group	Write	og* (p. 1467)		iam:PassRole
ModifyRecommendation	Grants permission to modify recommendation [permission only]	Write			
PromoteReadReplica	Grants permission to promote a Read Replica DB instance to a standalone DB instance	Write	db* (p. 1466)		
PromoteReadReplicaCluster	Grants permission to promote a Read Replica DB cluster to a standalone DB cluster	Write	cluster* (p. 1466)		
PurchaseReservedDBInstancesOffering	Grants permission to purchase a reserved DB instance offering	Write	ri* (p. 1467)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 1468) aws:TagKeys (p. 1468)	
RebootDBCluster	Grants permission to reboot a previously provisioned DB cluster	Write	cluster* (p. 1466)	rds:RebootDBInstance	
RebootDBInstance	Grants permission to restart the database engine service	Write	db* (p. 1466)		
RegisterDBProxyTarget	Grants permission to add targets to a database proxy target group	Write	target-group* (p. 1468)		
RemoveFromGlobal Aurora	Grants permission to detach an Aurora secondary cluster from an Aurora global database cluster	Write	cluster* (p. 1466) global-cluster* (p. 1467)		
RemoveRoleFromCluster	Grants permission to dissociate an AWS Identity and Access Management (IAM) role from an Amazon Aurora DB cluster	Write	cluster* (p. 1466)	iam:PassRole	
RemoveRoleFromDB	Grants permission to dissociate an AWS Identity and Access Management (IAM) role from a DB instance	Write	db* (p. 1466)	iam:PassRole	
RemoveSourceIdentifier	Grants permission to remove an source identifier from an existing RDS event notification subscription	Write	es* (p. 1467)		
RemoveTagsFromResource	Grants permission to remove Metadata tags from an Amazon RDS resource	Tagging	cev (p. 1468)		
			cluster (p. 1466)		
			cluster-endpoint (p. 1466)		
			cluster-pg (p. 1466)		
			cluster-snapshot (p. 1466)		
			db (p. 1466)		
			es (p. 1467)		
			og (p. 1467)		
			pg (p. 1467)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			proxy (p. 1467) proxy-endpoint (p. 1467) ri (p. 1467) secgrp (p. 1467) snapshot (p. 1467) subgrp (p. 1468) target-group (p. 1468)		
ResetDBClusterParameters	Grants permission to modify the parameters of a DB cluster parameter group to the default value	Write	cluster- pg* (p. 1466)		
ResetDBParameterGroups	Grants permission to modify the parameters of a DB parameter group to the engine/system default value	Write	pg* (p. 1467)		
RestoreDBClusterFromS3	Grants permission to create an Amazon Aurora DB cluster from data stored in an Amazon S3 bucket	Write	cluster* (p. 1466) cluster- pg* (p. 1466) og* (p. 1467) subgrp* (p. 1468)	iam:PassRole rds:AddTagsToResource	

Service Authorization Reference
Service Authorization Reference
Amazon RDS

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/\${TagKey} (p. 1468) aws:TagKeys (p. 1468) rds:req-tag/\${TagKey} (p. 1469) rds:DatabaseEngine (p. 1468) rds:DatabaseName (p. 1468) rds:StorageEncrypted (p. 1469)	
RestoreDBCluster	Grants permission to create a new DB cluster from a DB cluster snapshot	Write	cluster* (p. 1466) cluster-pg* (p. 1466) cluster-snapshot* (p. 1466) og* (p. 1467) subgrp* (p. 1468)	iam:PassRole rds:AddTagsToResource rds>CreateDBInstance	
				aws:RequestTag/\${TagKey} (p. 1468) aws:TagKeys (p. 1468) rds:req-tag/\${TagKey} (p. 1469) rds:DatabaseClass (p. 1468) rds:StorageSize (p. 1469) rds:Piops (p. 1468)	
RestoreDBClusterToPointInTime	Grants permission to restore a DB cluster to an arbitrary point in time	Write	cluster* (p. 1466) cluster-pg* (p. 1466) og* (p. 1467)	iam:PassRole rds:AddTagsToResource rds>CreateDBInstance	

Service Authorization Reference
Service Authorization Reference
Amazon RDS

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subgrp* (p. 1468)	aws:RequestTag/ \${TagKey} (p. 1468) aws:TagKeys (p. 1468) rds:req- tag/ \${TagKey} (p. 1469) rds:DatabaseClass (p. 1468) rds:StorageSize (p. 1469) rds:Piops (p. 1468)	
RestoreDBInstance	Creates a new DB instance from a DB snapshot	Write	db* (p. 1466) og* (p. 1467) pg* (p. 1467) snapshot* (p. 1467) subgrp* (p. 1468)	iam:PassRole rds:AddTagsToResource	rds:BackupTarget (p. 1468) aws:RequestTag/ \${TagKey} (p. 1468) aws:TagKeys (p. 1468) rds:req- tag/ \${TagKey} (p. 1469)
RestoreDBInstance	Creates a new DB instance from an Amazon S3 bucket	Write	db* (p. 1466) og* (p. 1467) pg* (p. 1467) subgrp* (p. 1468)	iam:PassRole rds:AddTagsToResource	

Service Authorization Reference
Service Authorization Reference
Amazon RDS

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 1468) aws:TagKeys (p. 1468) rds:req- tag/ \${TagKey} (p. 1469)	
RestoreDBInstanceToPointInTime	Grants permission to restore a DB instance to an arbitrary point in time	Write	db* (p. 1466) og* (p. 1467) pg* (p. 1467) subgrp* (p. 1468)		iam:PassRole rds:AddTagsToResource
					rds:BackupTarget (p. 1468) aws:RequestTag/ \${TagKey} (p. 1468) aws:TagKeys (p. 1468) rds:req- tag/ \${TagKey} (p. 1469)
RevokeDBSecurityGroupIngress	Grants permission to revoke ingress from a DBSecurityGroup for previously authorized IP ranges or EC2 or VPC Security Groups	Write	secgrp* (p. 1467)		
StartActivityStream	Grants permission to start Activity Stream	Write	cluster (p. 1466) db (p. 1466)		
StartDBCluster	Grants permission to start the DB cluster	Write	cluster* (p. 1466)		
StartDBInstance	Grants permission to start the DB instance	Write	db* (p. 1466)		
StartDBInstanceAutomatedBackups	Grants permission to start replication of automated backups to a different AWS Region	Write	db* (p. 1466)		
StartExportTask	Grants permission to start a new Export task for a DB snapshot	Write			iam:PassRole
StopActivityStream	Grants permission to stop Activity Stream	Write	cluster (p. 1466) db (p. 1466)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopDBCluster	Grants permission to stop the DB cluster	Write	cluster* (p. 1466)		
StopDBInstance	Grants permission to stop the DB instance	Write	db* (p. 1466)		
StopDBInstanceAutomatedBackupReplication	Grants permission to stop Automated Backup Replication for a DB instance	Write	db* (p. 1466)		

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 \(p. 1446\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1468) rds:cluster-tag/\${TagKey} (p. 1469)
cluster-endpoint	arn:\${Partition}:rds:\${Region}: \${Account}:cluster-endpoint: \${DbClusterEndpoint}	aws:ResourceTag/\${TagKey} (p. 1468)
cluster-pg	arn:\${Partition}:rds:\${Region}: \${Account}:cluster-pg: \${ClusterParameterGroupName}	aws:ResourceTag/\${TagKey} (p. 1468) rds:cluster-pg-tag/\${TagKey} (p. 1469)
cluster-snapshot	arn:\${Partition}:rds:\${Region}: \${Account}:cluster-snapshot: \${ClusterSnapshotName}	aws:ResourceTag/\${TagKey} (p. 1468) rds:cluster-snapshot-tag/\${TagKey} (p. 1469)
db	arn:\${Partition}:rds:\${Region}: \${Account}:db:\${DbInstanceName}	aws:ResourceTag/\${TagKey} (p. 1468) rds:DatabaseClass (p. 1468) rds:DatabaseEngine (p. 1468) rds:DatabaseName (p. 1468) rds:MultiAz (p. 1468)

Resource types	ARN	Condition keys
		rds:Piops (p. 1468) rds:StorageEncrypted (p. 1469) rds:StorageSize (p. 1469) rds:Vpc (p. 1469) rds:db-tag/ \${TagKey} (p. 1469)
es	<code>arn:\${Partition}:rds:\${Region}: \${Account}:es:\${SubscriptionName}</code>	aws:ResourceTag/ \${TagKey} (p. 1468) rds:es-tag/ \${TagKey} (p. 1469)
global-cluster	<code>arn:\${Partition}:rds::\${Account}:global-cluster:\${GlobalCluster}</code>	
og	<code>arn:\${Partition}:rds:\${Region}: \${Account}:og:\${OptionGroupName}</code>	aws:ResourceTag/ \${TagKey} (p. 1468) rds:og-tag/ \${TagKey} (p. 1469)
pg	<code>arn:\${Partition}:rds:\${Region}: \${Account}:pg:\${ParameterGroupName}</code>	aws:ResourceTag/ \${TagKey} (p. 1468) rds:pg-tag/ \${TagKey} (p. 1469)
proxy	<code>arn:\${Partition}:rds:\${Region}: \${Account}:db-proxy:\${DbProxyId}</code>	aws:ResourceTag/ \${TagKey} (p. 1468)
proxy-endpoint	<code>arn:\${Partition}:rds:\${Region}: \${Account}:db-proxy-endpoint: \${DbProxyEndpointId}</code>	aws:ResourceTag/ \${TagKey} (p. 1468)
ri	<code>arn:\${Partition}:rds:\${Region}: \${Account}:ri:\${ReservedDbInstanceName}</code>	aws:ResourceTag/ \${TagKey} (p. 1468) rds:ri-tag/ \${TagKey} (p. 1469)
secgrp	<code>arn:\${Partition}:rds:\${Region}: \${Account}:secgrp:\${SecurityGroupName}</code>	aws:ResourceTag/ \${TagKey} (p. 1468) rds:secgrp-tag/ \${TagKey} (p. 1469)
snapshot	<code>arn:\${Partition}:rds:\${Region}: \${Account}:snapshot:\${SnapshotName}</code>	aws:ResourceTag/ \${TagKey} (p. 1468) rds:snapshot-tag/ \${TagKey} (p. 1469)

Resource types	ARN	Condition keys
subgrp	arn:\${Partition}:rds:\${Region}: \${Account}:subgrp:\${SubnetGroupName}	aws:ResourceTag/\${TagKey} (p. 1468) rds:subgrp-tag/\${TagKey} (p. 1469)
target	arn:\${Partition}:rds:\${Region}: \${Account}:target:\${TargetId}	
target-group	arn:\${Partition}:rds:\${Region}: \${Account}:target-group:\${TargetGroupId}	aws:ResourceTag/\${TagKey} (p. 1468)
cev	arn:\${Partition}:rds:\${Region}: \${Account}:cev:\${Engine}/\${EngineVersion}/ \${CustomDbEngineVersionId}	aws:ResourceTag/\${TagKey} (p. 1468)

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 [Available global condition 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: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: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	Numeric

Condition keys	Description	Type
	indicate a DB instance that does not have PIOPS enabled, specify 0	
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:Vpc	Filters access by the value that specifies whether the DB instance runs in an Amazon Virtual Private Cloud (Amazon VPC). To indicate that the DB instance runs in an Amazon VPC, specify true	Bool
rds:cluster-pg-tag/\${TagKey}	Filters access by the tag attached to a DB cluster parameter group	String
rds:cluster-snapshot-tag/\${TagKey}	Filters access by the tag attached to a DB cluster snapshot	String
rds:cluster-tag/\${TagKey}	Filters access by the tag attached to a DB cluster	String
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 \(p. 1470\)](#)
- [Resource types defined by Amazon RDS Data API \(p. 1471\)](#)
- [Condition keys for Amazon RDS Data API \(p. 1471\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1471)		
			aws:ResourceTag/ \${TagKey} (p. 1471)		
			aws:TagKeys (p. 1472)		
BeginTransaction	Grants permission to start a SQL transaction	Write	cluster* (p. 1471)		
			aws:ResourceTag/ \${TagKey} (p. 1471)		
			aws:TagKeys (p. 1472)		
CommitTransaction	Grants permission to end a SQL transaction started with the <code>BeginTransaction</code> operation and commits the changes	Write	cluster* (p. 1471)	rds-data:BeginTransaction	
			aws:ResourceTag/ \${TagKey} (p. 1471)		
			aws:TagKeys (p. 1472)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ExecuteSql	Grants permission to run one or more SQL statements. This operation is deprecated. Use the BatchExecuteStatement or ExecuteStatement operation	Write	cluster* (p. 1471)		
				aws:ResourceTag/ \${TagKey} (p. 1471)	aws:TagKeys (p. 1472)
ExecuteStatement	Grants permission to run a SQL statement against a database	Write	cluster* (p. 1471)		
				aws:ResourceTag/ \${TagKey} (p. 1471)	aws:TagKeys (p. 1472)
RollbackTransaction	Grants permission to perform a rollback of a transaction. Rolling back a transaction cancels its changes	Write	cluster* (p. 1471)		rds-data:BeginTransaction
				aws:ResourceTag/ \${TagKey} (p. 1471)	aws:TagKeys (p. 1472)

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 \(p. 1470\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
<code>cluster</code>	<code>arn:\${Partition}:rds:\${Region}: \${Account}:cluster:\${DbClusterInstanceName}</code>	aws:ResourceTag/ \${TagKey} (p. 1471) aws:TagKeys (p. 1472)

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:ResourceTag/ \${TagKey}</code>	Filters access by the tags associated with the resource	String

Condition keys	Description	Type
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 \(p. 1472\)](#)
- [Resource types defined by Amazon RDS IAM Authentication \(p. 1472\)](#)
- [Condition keys for Amazon RDS IAM Authentication \(p. 1473\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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	db-management user* (p. 1473)		

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 \(p. 1472\)](#) identifies the resource

types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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 [Available keys for conditions](#).

Actions, resources, and condition keys for Recycle Bin

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 Recycle Bin \(p. 1473\)](#)
- [Resource types defined by Recycle Bin \(p. 1474\)](#)
- [Condition keys for Recycle Bin \(p. 1475\)](#)

Actions defined by 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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1474)		
				aws:RequestTag/ \${TagKey} (p. 1475) aws:TagKeys (p. 1475)	
DeleteRule	Grants permission to delete a Recycle Bin retention rule	Write	rule* (p. 1474)		
GetRule	Grants permission to get detailed information about a Recycle Bin retention rule	Read	rule* (p. 1474)		
				aws:ResourceTag/ \${TagKey} (p. 1475)	
ListRules	Grants permission to list the Recycle Bin retention rules in the Region	Read			
ListTagsForResource	Grants permission to list the tags associated with a resource	Read	rule* (p. 1474)		
TagResource	Grants permission to add or update tags of a resource	Tagging	rule* (p. 1474)		
				aws:RequestTag/ \${TagKey} (p. 1475) aws:TagKeys (p. 1475)	
UntagResource	Grants permission to remove tags associated with a resource	Tagging	rule* (p. 1474)		
				aws:RequestTag/ \${TagKey} (p. 1475) aws:TagKeys (p. 1475)	
UpdateRule	Grants permission to update an existing Recycle Bin retention rule	Write	rule* (p. 1474)		

Resource types defined by 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 \(p. 1473\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1475)

Condition keys for Recycle Bin

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 [Available global condition keys](#).

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

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 \(p. 1475\)](#)
- [Resource types defined by Amazon Redshift \(p. 1488\)](#)
- [Condition keys for Amazon Redshift \(p. 1490\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1488)		
AuthorizeClusterSubnetIngress	Grants permission to add an subnet (ingress) rule to an Amazon Redshift security group	Write	securitygroup* (p. 1489)		
AuthorizeDataShareConsumer	Grants permission to authorize the specified datashare consumer to consume a datashare		securitygroupingress-ec2securitygroup* (p. 1489)		
AuthorizeEndpoint	Grants permission to authorize endpoint related activities for redshift-managed vpc endpoint	Permissions management	datashare* (p. 1488)		redshift:ConsumerIdentifier (p. 1490)
AuthorizeSnapshotRestore	Grants permission to the specified AWS account to restore a snapshot	Permissions management			
BatchDeleteClusterSnapshots	Grants permission to delete snapshots in a batch of size upto 100	Write	snapshot* (p. 1489)		
BatchModifyClusterSettings	Grants permission to modify settings for a list of snapshots	Write	snapshot* (p. 1489)		
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* (p. 1488)		
CopyClusterSnapshot	Grants permission to copy a cluster snapshot	Write	snapshot* (p. 1489)		
				aws:RequestTag/\${TagKey} (p. 1490)	aws:TagKeys (p. 1490)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAuthenticator	Grants permission to create an Amazon Redshift authentication profile	Write			
CreateCluster	Grants permission to create a cluster	Write	cluster* (p. 1488)		
				aws:RequestTag/ \${TagKey} (p. 1490)	aws:TagKeys (p. 1490)
CreateClusterParameterGroup	Grants permission to create an Amazon Redshift parameter group	Write	parametergroup* (p. 1489)		
				aws:RequestTag/ \${TagKey} (p. 1490)	aws:TagKeys (p. 1490)
CreateClusterSecurityGroup	Grants permission to create an Amazon Redshift security group	Write	securitygroup* (p. 1489)		
				aws:RequestTag/ \${TagKey} (p. 1490)	aws:TagKeys (p. 1490)
CreateClusterSnapshot	Grants permission to create a manual snapshot of the specified cluster	Write	snapshot* (p. 1489)		
				aws:RequestTag/ \${TagKey} (p. 1490)	aws:TagKeys (p. 1490)
CreateClusterSubnetGroup	Grants permission to create an Amazon Redshift subnet group	Write	subnetgroup* (p. 1489)		
				aws:RequestTag/ \${TagKey} (p. 1490)	aws:TagKeys (p. 1490)
CreateClusterUser	Grants permission to automatically create the specified Amazon Redshift user if it does not exist	Permissions management	dbuser* (p. 1489)		
				redshift:DbUser (p. 1490)	
CreateEndpointAssociation	Grants permission to create a redshift-managed vpc endpoint	Write			
CreateEventSubscription	Grants permission to create an Amazon Redshift event notification subscription	Write	eventsSubscription* (p. 1489)		
				aws:RequestTag/ \${TagKey} (p. 1490)	aws:TagKeys (p. 1490)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateHsmClientCertificate	Grants permission to create an HSM client certificate that a cluster uses to connect to an HSM	Write	hsmclientcertificate* (p. 1489) aws:RequestTag/ \${TagKey} (p. 1490) aws:TagKeys (p. 1490)		
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* (p. 1489) aws:RequestTag/ \${TagKey} (p. 1490) aws:TagKeys (p. 1490)		
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* (p. 1489) aws:RequestTag/ \${TagKey} (p. 1490) aws:TagKeys (p. 1490)		
CreateSnapshotSchedule	Grants permission to create a snapshot schedule	Write	snapshotschedule* (p. 1489) aws:RequestTag/ \${TagKey} (p. 1490) aws:TagKeys (p. 1490)		
CreateTags	Grants permission to add one or more tags to a specified resource	Tagging	cluster (p. 1488) dbgroup (p. 1489) dbname (p. 1489) dbuser (p. 1489) eventsSubscription (p. 1489) hsmclientcertificate (p. 1489) hsmconfiguration (p. 1489) parametergroup (p. 1489) securitygroup (p. 1489) securitygroupingress-cidr (p. 1489)		

Service Authorization Reference
Service Authorization Reference
Amazon Redshift

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			securitygroupingress-ec2securitygroup (p. 1489) snapshot (p. 1489) snapshotcopygrant (p. 1489) snapshotschedule (p. 1489) subnetgroup (p. 1489) usagelimit (p. 1489)		aws:RequestTag/ {\$TagKey} (p. 1490) aws:TagKeys (p. 1490)
CreateUsageLimit	Grants permission to create a usage limit	Write	usagelimit* (p. 1489)		aws:RequestTag/ {\$TagKey} (p. 1490) aws:TagKeys (p. 1490)
DeauthorizeDataShare	Grants permission to remove permission from the specified datashare consumer to consume a datashare	Permissions management	datashare* (p. 1488)		redshift:ConsumerIdentifier (p. 1490)
DeleteAuthenticationProfile	Grants permission to delete an Amazon Redshift authentication profile	Write			
DeleteCluster	Grants permission to delete a previously provisioned cluster	Write	cluster* (p. 1488)		
DeleteClusterParameterGroup	Grants permission to delete an Amazon Redshift parameter group	Write	parametergroup* (p. 1489)		
DeleteClusterSecurityGroup	Grants permission to delete an Amazon Redshift security group	Write	securitygroup* (p. 1489)		
DeleteClusterSnapshot	Grants permission to delete a manual snapshot	Write	snapshot* (p. 1489)		
DeleteClusterSubnetGroup	Grants permission to delete a subnet group	Write	subnetgroup* (p. 1489)		
DeleteEndpointAssociation	Grants permission to delete a redshift-managed vpc endpoint	Write			
DeleteEventSubscription	Grants permission to delete an Amazon Redshift event notification subscription	Write	eventsSubscription* (p. 1489)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteHsmClientCertificate	Grants permission to delete an HSM client certificate	Write	hsmclientcertificate* (p. 1489)		
DeleteHsmConfiguration	Grants permission to delete an Amazon Redshift HSM configuration	Write	hsmconfiguration* (p. 1489)		
DeletePartner	Grants permission to delete a partner integration from a cluster	Write			
DeleteSavedQuery [permission only]	Grants permission to delete saved SQL queries through the Amazon Redshift console	Write			
DeleteScheduledAction	Grants permission to delete an Amazon Redshift scheduled action	Write			
DeleteSnapshotCopyGrant	Grants permission to delete a snapshot copy grant	Write	snapshotcopygrant* (p. 1489)		
DeleteSnapshotSchedule	Grants permission to delete a snapshot schedule	Write	snapshotschedule* (p. 1489)		
DeleteTags	Grants permission to delete a tag or tags from a resource	Tagging	cluster (p. 1488)		
dbgroup (p. 1489)					
dbname (p. 1489)					
dbuser (p. 1489)					
eventsSubscription (p. 1489)					
hsmclientcertificate (p. 1489)					
hsmconfiguration (p. 1489)					
parametergroup (p. 1489)					
securitygroup (p. 1489)					
securitygroupingress-cidr (p. 1489)					
securitygroupingress-ec2SecurityGroup (p. 1489)					
snapshot (p. 1489)					
snapshotcopygrant (p. 1489)					
snapshotschedule (p. 1489)					
subnetgroup (p. 1489)					

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			usagelimit (p. 1489)		
			aws:TagKeys (p. 1490)		
DeleteUsageLimit	Grants permission to delete a usage limit	Write	usagelimit* (p. 1489)		
DescribeAccountAttributes	Grants permission to describe attributes attached to the specified AWS account	Read			
DescribeAuthenticationProfiles	Grants permission to describe authentication profiles	Read			
DescribeClusterDatabaseRevisions	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	parametergroup* (p. 1489)		
DescribeClusterSecurityGroups	Grants permission to describe Amazon Redshift security groups	Read			
DescribeClusterSnapshots	Grants permission to describe one or more snapshot objects, which contain metadata about your cluster snapshots	Read			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDataShares	Grants permission to describe datashares created and consumed by your clusters	Read			
DescribeDataSharesForClusters	Grants permission to describe only datashares consumed by your clusters	Read			
DescribeDataSharesForParameters	Grants permission to describe only datashares created by your clusters	Read			
DescribeDefaultClusterParameters	Grants permission to describe parameter settings for a parameter group family	Read			
DescribeEndpoint	Grants permission to describe Redshift -managed vpc endpoints	Read			
DescribeEndpointAuthorization	Grants permission to authorize describe activity for redshift-managed vpc endpoint		Permissions management		
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			
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			
DescribeLoggingStatus	Grants permission to describe whether information, such as queries and connection attempts, is being logged for a cluster	Read	cluster* (p. 1488)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeNodeConfigurations	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			
DescribeQuery [permission only]	Grants permission to describe a query through the Amazon Redshift console	Read			
DescribeReservedExchangeStatusDetails	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* (p. 1488)		
DescribeSavedQueries [permission only]	Grants permission to describe saved queries through the Amazon Redshift console	Read			
DescribeScheduledActions	Grants permission to describe created Amazon Redshift scheduled actions	Read			
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* (p. 1489)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 one or more table restore requests made using the RestoreTableFromClusterSnapshot API action	Read			
DescribeTags	Grants permission to describe tags	Read	cluster (p. 1488) dbgroup (p. 1489) dbname (p. 1489) dbuser (p. 1489) eventsSubscription (p. 1489) hsmClientCertificate (p. 1489) hsmConfiguration (p. 1489) parameterGroup (p. 1489) securityGroup (p. 1489) securityGroupIngress-cidr (p. 1489) securityGroupIngress-ec2SecurityGroup (p. 1489) snapshot (p. 1489) snapshotCopyGrant (p. 1489) snapshotSchedule (p. 1489) subnetGroup (p. 1489) usageLimit (p. 1489)		
DescribeUsageLimits	Grants permission to describe usage limits	Read	usageLimit* (p. 1489)		
DisableLogging	Grants permission to disable logging information, such as queries and connection attempts, for a cluster	Write	cluster* (p. 1488)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableSnapshotCopy	Grants permission to disable the automatic copy of snapshots for a cluster	Write	cluster* (p. 1488)		
DisassociateDataShareConsumer	Grants permission to disassociate a consumer from a datashare	Write	datashare* (p. 1488)		
EnableLogging	Grants permission to enable logging information, such as queries and connection attempts, for a cluster	Write	cluster* (p. 1488)		
EnableSnapshotCopy	Grants permission to enable the automatic copy of snapshots for a cluster	Write	cluster* (p. 1488)		
ExecuteQuery [permission only]	Grants permission to execute a query through the Amazon Redshift console	Write			
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* (p. 1489) dbgroup (p. 1489) dbname (p. 1489)		
				redshift:DbName (p. 1490) redshift:DbUser (p. 1490) redshift:DurationSeconds (p. 1490)	
GetReservedNodeConfigurationOptions	Grants permission to get the configuration options for the reserved-node exchange	Read			
GetReservedNodeOfferings	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			
JoinGroup	Grants permission to join the specified Amazon Redshift group	Permissions management	dbgroup* (p. 1489)		
ListDatabases [permission only]	Grants permission to list databases through the Amazon Redshift console	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
ModifyAquaConfig	Grants permission to modify the AQUA configuration of a cluster	Write	cluster* (p. 1488)		
ModifyAuthenticationProfile	Grants permission to modify an existing Amazon Redshift authentication profile	Write			
ModifyCluster	Grants permission to modify the settings of a cluster	Write	cluster* (p. 1488)		
ModifyClusterDbRevision	Grants permission to modify the database revision of a cluster	Write	cluster* (p. 1488)		
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* (p. 1488)		
ModifyClusterMaintenance	Grants permission to modify the maintenance settings of a cluster	Write			
ModifyClusterParameterGroup	Grants permission to modify the parameters of a parameter group	Write	parametergroup* (p. 1489)		
ModifyClusterSnapshot	Grants permission to modify the settings of a snapshot	Write	snapshot* (p. 1489)		
ModifyClusterSnapshotSchedule	Grants permission to modify a snapshot schedule for a cluster	Write	cluster* (p. 1488)		
ModifyClusterSubnetGroup	Grants permission to modify a cluster subnet group to include the specified list of VPC subnets	Write	subnetgroup* (p. 1489)		
ModifyEndpoint	Grants permission to modify a redshift-managed vpc endpoint	Write			
ModifyEventSubscription	Grants permission to modify an existing Amazon Redshift event notification subscription	Write	eventsSubscription* (p. 1489)		

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				
ModifySnapshotCopyRequest	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* (p. 1488)			
ModifySnapshotSchedule	Grants permission to modify a snapshot schedule	Write	snapshotSchedule* (p. 1489)			
ModifyUsageLimit	Grants permission to modify a usage limit	Write	usageLimit* (p. 1489)			
PauseCluster	Grants permission to pause a cluster	Write	cluster* (p. 1488)			
PurchaseReservedNodeOffering	Grants permission to purchase a reserved node	Write				
RebootCluster	Grants permission to reboot a cluster	Write	cluster* (p. 1488)			
RejectDataShare	Grants permission to decline a datashare shared from another account	Permissions management	datashare* (p. 1488)			
ResetClusterParameter	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* (p. 1489)			
ResizeCluster	Grants permission to change the size of a cluster	Write	cluster* (p. 1488)			
RestoreFromClusterSnapshot	Grants permission to create a cluster from a snapshot	Write	cluster* (p. 1488)			
			snapshot* (p. 1489)		aws:RequestTag/ {\$TagKey} (p. 1490)	
RestoreTableFromSnapshot	Grants permission to create a table from a table in an Amazon Redshift cluster snapshot		Write	cluster* (p. 1488)		
				snapshot* (p. 1489)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ResumeCluster	Grants permission to resume a cluster	Write	cluster* (p. 1488)		
RevokeClusterSecurityGroupAccess	Grants permission to revoke security group access from an Amazon Redshift security group for a previously authorized IP range or Amazon EC2 security group	Write	securitygroup* (p. 1489)		
			securitygroupingress-ec2securitygroup* (p. 1489)		
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* (p. 1489)		
RotateEncryptionKey	Grants permission to rotate an encryption key for a cluster	Write	cluster* (p. 1488)		
UpdatePartnerStatus	Grants permission to update the status of a partner integration	Write			
ViewQueriesFromResults [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 \(p. 1475\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
cluster	<code>arn:\${Partition}:redshift:\${Region}:\${Account}:cluster:\${ClusterName}</code>	aws:ResourceTag/\${TagKey} (p. 1490)
datashare	<code>arn:\${Partition}:redshift:\${Region}:\${Account}:datashare:\${ProducerClusterNamespace}/\${DataShareName}</code>	aws:ResourceTag/\${TagKey} (p. 1490)

Resource types	ARN	Condition keys
dbgroup	arn:\${Partition}:redshift:\${Region}: \${Account}:dbgroup:\${ClusterName}/\${DbGroup}	aws:ResourceTag/ \${TagKey} (p. 1490)
dbname	arn:\${Partition}:redshift:\${Region}: \${Account}:dbname:\${ClusterName}/\${DbName}	aws:ResourceTag/ \${TagKey} (p. 1490)
dbuser	arn:\${Partition}:redshift:\${Region}: \${Account}:dbuser:\${ClusterName}/\${DbUser}	aws:ResourceTag/ \${TagKey} (p. 1490)
eventsSubscription	arn:\${Partition}:redshift:\${Region}: \${Account}:eventsSubscription: \${EventSubscriptionName}	aws:ResourceTag/ \${TagKey} (p. 1490)
hsmclientcertificate	arn:\${Partition}:redshift:\${Region}: \${Account}:hsmclientcertificate: \${HSMClientCertificateId}	aws:ResourceTag/ \${TagKey} (p. 1490)
hsmconfiguration	arn:\${Partition}:redshift:\${Region}: \${Account}:hsmconfiguration: \${HSMConfigurationId}	aws:ResourceTag/ \${TagKey} (p. 1490)
parametergroup	arn:\${Partition}:redshift: \${Region}:\${Account}:parametergroup: \${ParameterGroupName}	aws:ResourceTag/ \${TagKey} (p. 1490)
securitygroup	arn:\${Partition}:redshift: \${Region}: \${Account}:securitygroup: \${SecurityGroupName}/ec2securitygroup/ \${Owner}/\${Ec2SecurityGroupId}	aws:ResourceTag/ \${TagKey} (p. 1490)
securitygroupingresscidr	arn:\${Partition}:redshift:\${Region}: \${Account}:securitygroupingress: \${SecurityGroupName}/cidrip/\${IpRange}	aws:ResourceTag/ \${TagKey} (p. 1490)
securitygroupingressec2securitygroup	arn:\${Partition}:redshift:\${Region}: \${Account}:securitygroupingress: \${SecurityGroupName}/ec2securitygroup/ \${Owner}/\${Ece2SecuritygroupId}	aws:ResourceTag/ \${TagKey} (p. 1490)
snapshot	arn:\${Partition}:redshift:\${Region}: \${Account}:snapshot:\${ClusterName}/ \${SnapshotName}	aws:ResourceTag/ \${TagKey} (p. 1490)
snapshotcopygrant	arn:\${Partition}:redshift:\${Region}: \${Account}:snapshotcopygrant: \${SnapshotCopyGrantName}	aws:ResourceTag/ \${TagKey} (p. 1490)
snapshotschedule	arn:\${Partition}:redshift:\${Region}: \${Account}:snapshotschedule: \${ParameterGroupName}	aws:ResourceTag/ \${TagKey} (p. 1490)
subnetgroup	arn:\${Partition}:redshift:\${Region}: \${Account}:subnetgroup:\${SubnetGroupName}	aws:ResourceTag/ \${TagKey} (p. 1490)
usagelimit	arn:\${Partition}:redshift:\${Region}: \${Account}:usagelimit:\${UsageLimitId}	aws:ResourceTag/ \${TagKey} (p. 1490)

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters access by actions based on the allowed set of values for each of the tags	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters access by actions based on tag-value associated with the resource	String
<code>aws:TagKeys</code>	Filters access by actions based on the presence of mandatory tags in the request	String
<code>redshift:ConsumerIdentifier</code>	Filters access by the datashare consumer	String
<code>redshift:DbName</code>	Filters access by the database name	String
<code>redshift:DbUser</code>	Filters access by the database user name	String
<code>redshift:DurationSeconds</code>	Filters access by the number of seconds until a temporary credential set expires	String

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 \(p. 1490\)](#)
- [Resource types defined by Amazon Redshift Data API \(p. 1492\)](#)
- [Condition keys for Amazon Redshift Data API \(p. 1492\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1492)		
CancelStatement	Grants permission to cancel a running query	Write		redshift-data:statement-owner-iam-userid (p. 1492)	
DescribeStatement	Grants permission to retrieve detailed information about a statement execution	Read		redshift-data:statement-owner-iam-userid (p. 1492)	
DescribeTable	Grants permission to retrieve metadata about a particular table	Read	cluster* (p. 1492)		
ExecuteStatement	Grants permission to execute a query	Write	cluster* (p. 1492)		
GetStatementResult	Grants permission to fetch the result of a query	Read		redshift-data:statement-owner-iam-userid (p. 1492)	
ListDatabases	Grants permission to list databases for a given cluster	Read	cluster* (p. 1492)		
ListSchemas	Grants permission to list schemas for a given cluster	Read	cluster* (p. 1492)		
ListStatements	Grants permission to list queries for a given principal	List		redshift-data:statement-owner-iam-userid (p. 1492)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTables	Grants permission to list tables for a given cluster	List	cluster* (p. 1492)		

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 \(p. 1490\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
cluster	<code>arn:\${Partition}:redshift:\${Region}:\${Account}:cluster:\${ClusterName}</code>	<code>aws:ResourceTag/\${TagKey}</code> (p. 1492)

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:ResourceTag/\${TagKey}</code>	Filters actions based on tag-value associated with the resource	String
<code>redshift-data:statement-owner-iam-userid</code>	Filters access by statement owner iam userid	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 \(p. 1493\)](#)
- [Resource types defined by Amazon Rekognition \(p. 1498\)](#)
- [Condition keys for Amazon Rekognition \(p. 1498\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CompareFaces	Grants permission to compare faces in the source input image with each face detected in the target input image	Read			
CreateCollection	Grants permission to create a collection in an AWS Region	Write		aws:RequestTag/\${TagKey} (p. 1498) aws:TagKeys (p. 1498)	
CreateDataset	Grants permission to create a new Amazon Rekognition Custom Labels dataset	Write	project* (p. 1498)		
CreateProject	Grants permission to create an Amazon Rekognition Custom Labels project	Write	project* (p. 1498)		
CreateProjectVersion	Grants permission to begin training a new version of a model	Write	project* (p. 1498)		
CreateStreamProcessor	Grants permission to create an Amazon Rekognition stream processor	Write	collection* (p. 1498)		
				aws:RequestTag/\${TagKey} (p. 1498) aws:TagKeys (p. 1498)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteCollection	Grants permission to delete the specified collection	Write	collection* (p. 1498)		
DeleteDataset	Grants permission to delete an existing Amazon Rekognition Custom Labels dataset	Write	dataset* (p. 1498)		
DeleteFaces	Grants permission to delete faces from a collection	Write	collection* (p. 1498)		
DeleteProject	Grants permission to delete a project	Write	project* (p. 1498)		
DeleteProjectVersion	Grants permission to delete a model	Write	projectversion* (p. 1498)		
DeleteStreamProcessor	Grants permission to delete the specified stream processor	Write	streamprocessor* (p. 1498)		
DescribeCollection	Grants permission to read details about a collection	Read	collection* (p. 1498)		
DescribeDataset	Grants permission to describe an Amazon Rekognition Custom Labels dataset	Read	dataset* (p. 1498)		
DescribeProjectVersion	Grants permission to list the versions of a model in an Amazon Rekognition Custom Labels project	Read	project* (p. 1498)		
DescribeProjects	Grants permission to list Amazon Rekognition Custom Labels projects	Read			
DescribeStreamProcessor	Grants permission to get information about the specified stream processor	Read	streamprocessor* (p. 1498)		
DetectCustomLabel	Grants permission to detect custom labels in a supplied image	Read	projectversion* (p. 1498)		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DetectProtectiveEquipment	Grants permission to detect 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			
DistributeDatasetEntries	Grants permission to distribute the entries in a training dataset across the training dataset and the test dataset for a project	Write	dataset* (p. 1498)		
GetCelebrityInfo	Grants permission to read the name, and additional information, of a celebrity	Read			
GetCelebrityRecognitionResults	Grants permission to read the celebrity recognition results found in a stored video by an asynchronous celebrity recognition job	Read			
GetContentModerationAnalysisResults	Grants permission to read the content moderation analysis results found in a stored video by an asynchronous content moderation job	Read			
GetFaceDetectionResults	Grants permission to read the faces detection results found in a stored video by an asynchronous face detection job	Read			
GetFaceSearchResults	Grants permission to read the matching collection faces found in a stored video by an asynchronous face search job	Read			
GetLabelDetectionResults	Grants permission to read the label detected results found in a stored video by an asynchronous label detection job	Read			
GetPersonTrackingResults	Grants permission to read the list of persons detected in a stored video by an asynchronous person tracking job	Read			
GetSegmentDetectionResults	Grants permission to get the video segments found in a stored video by an asynchronous segment detection job	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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* (p. 1498)		
ListCollections	Grants permission to read the collection Id's in your account	Read	collection* (p. 1498)		
ListDatasetEntries	Grants permission to list the dataset entries in an existing Amazon Rekognition Custom Labels dataset	Read	dataset* (p. 1498)		
ListDatasetLabels	Grants permission to list the labels in a dataset	Read	dataset* (p. 1498)		
ListFaces	Grants permission to read metadata for faces in the specified collection	Read	collection* (p. 1498)		
ListStreamProcessors	Grants permission to get a list of your stream processors	List	streamprocessor* (p. 1498)		
ListTagsForResource	Grants permission to return a list of tags associated with a resource	Read	projectversion* (p. 1498)		
RecognizeCelebrities	Grants permission to detect celebrities in the input image	Read			
SearchFaces	Grants permission to search the specified collection for the supplied face ID	Read	collection* (p. 1498)		
SearchFacesByImage	Grants permission to search the specified collection for the largest face in the input image	Read	collection* (p. 1498)		
StartCelebrityRecognition	Grants permission to start the asynchronous recognition of celebrities in a stored video	Write			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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* (p. 1498)		
StartLabelDetection	Grants permission to start asynchronous detection of labels in a stored video	Write			
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* (p. 1498)		
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* (p. 1498)		
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* (p. 1498)		
StopStreamProcessor	Grants permission to stop a running stream processor	Write	streamprocessor* (p. 1498)		
TagResource	Grants permission to add one or more tags to a resource	Tagging	collection (p. 1498)		
projectversion (p. 1498)					
streamprocessor (p. 1498)					
aws:RequestTag/ \${TagKey} (p. 1498)	aws:TagKeys (p. 1498)				
UntagResource	Grants permission to remove one or more tags from a resource	Tagging	collection (p. 1498)		
projectversion (p. 1498)					
streamprocessor (p. 1498)					
	aws:TagKeys (p. 1498)				
UpdateDatasetEntries	Grants permission to add or update one or more JSON Lines (entries) in a dataset	Write	dataset* (p. 1498)		

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 \(p. 1493\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
<code>collection</code>	<code>arn:\${Partition}:rekognition:\${Region}:\${Account}:collection/\${CollectionId}</code>	
<code>streamprocessor</code>	<code>arn:\${Partition}:rekognition:\${Region}:\${Account}:streamprocessor/\${StreamprocessorId}</code>	
<code>project</code>	<code>arn:\${Partition}:rekognition:\${Region}:\${Account}:project/\${ProjectName}/\${CreationTimestamp}</code>	
<code>projectversion</code>	<code>arn:\${Partition}:rekognition:\${Region}:\${Account}:project/\${ProjectName}/version/\${VersionName}/\${CreationTimestamp}</code>	
<code>dataset</code>	<code>arn:\${Partition}:rekognition:\${Region}:\${Account}:project/\${ProjectName}/dataset/\${DatasetType}/\${CreationTimestamp}</code>	

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 [Available global condition keys](#).

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

Actions, resources, and condition keys for AWS Resilience Hub Service

AWS Resilience Hub Service (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 Service \(p. 1499\)](#)
- [Resource types defined by AWS Resilience Hub Service \(p. 1503\)](#)
- [Condition keys for AWS Resilience Hub Service \(p. 1504\)](#)

Actions defined by AWS Resilience Hub 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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddDraftAppVersion	Grants permission to add draft application version resource mappings	Write	application* (p. 1504)		cloudformation:DescribeStacks cloudformation>ListStacks resource-groups:ListGroupResources servicecatalog:GetApplication servicecatalog>ListAssociations
CreateApp	Grants permission to create application	Write	resiliency-policy (p. 1503)		
				aws:RequestTag/\${TagKey} (p. 1504) aws:TagKeys (p. 1504)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRecommendationTemplate	Grants permission to create recommendation template	Write	application* (p. 1504)		s3:CreateBucket s3>ListBucket s3:PutObject
				aws:RequestTag/ \${TagKey} (p. 1504) aws:TagKeys (p. 1504)	
CreateResiliencyPolicy	Grants permission to create resiliency policy	Write		aws:RequestTag/ \${TagKey} (p. 1504) aws:TagKeys (p. 1504)	
DeleteApp	Grants permission to batch delete application	Write	application* (p. 1504)		
DeleteAppAssessment	Grants permission to batch delete application assessment	Write	application* (p. 1504)		
DeleteRecommendationTemplate	Grants permission to batch delete recommendation template	Write	application* (p. 1504)		
DeleteResiliencyPolicy	Grants permission to batch delete resiliency policy	Write	resiliency- policy* (p. 1503)		
DescribeApp	Grants permission to describe application	Read	application* (p. 1504)		
DescribeAppAssessment	Grants permission to describe application assessment	Read	application* (p. 1504)		
DescribeAppVersion	Grants permission to describe application resolution status	Read	application* (p. 1504)		
DescribeAppVersionTemplate	Grants permission to describe application template	Read	application* (p. 1504)		
DescribeDraftAppVersionStatus	Grants permission to describe draft application version resources import status	Read	application* (p. 1504)		
DescribeResiliencyPolicy	Grants permission to describe resiliency policy	Read	resiliency- policy* (p. 1503)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportResourcesToAppDraft	Grants permission to import resources to draft application version	Write	application* (p. 1504)		cloudformation:DescribeStacks cloudformation>ListStacks resource-groups:GetGroup resource-groups>ListGroupResources servicecatalog:GetApplicationAssociations servicecatalog>ListAssociations
ListAlarmRecommendations	Grants permission to list alarm recommendation	List	application* (p. 1504)		
ListAppAssessments	Grants permission to list application assessment	List	application (p. 1504)		
ListAppComponentRecommendations	Grants permission to list app component recommendations	List	application* (p. 1504)		
ListAppVersionResponseMappings	Grants permission to application version response mappings	List	application* (p. 1504)		
ListAppVersionResources	Grants permission to list application resources	List	application* (p. 1504)		
ListAppVersions	Grants permission to list application version	List	application* (p. 1504)		
ListApps	Grants permission to list applications	List			
ListRecommendationTemplates	Grants permission to list recommendation templates	List	application* (p. 1504)		
ListResiliencyPolicies	Grants permission to list resiliency policies	List			
ListSopRecommendations	Grants permission to list SOP recommendations	List	application* (p. 1504)		
ListSuggestedResiliencyPolicies	Grants permission to list suggested resilience policies	List			
ListTagsForResource	Grants permission to list tags for a resource	Read			
ListTestRecommendations	Grants permission to list test recommendations	List	application* (p. 1504)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListUnsupportedAppVersions	Grants permission to list application version resources	List	application* (p. 1504)		
PublishAppVersion	Grants permission to publish application version	Write	application* (p. 1504)		
PutDraftAppVersion	Grants permission to put draft application version template	Write	application* (p. 1504)		
RemoveDraftAppVersionMappings	Grants permission to remove draft application version mappings	Write	application* (p. 1504)		
ResolveAppVersionMappings	Grants permission to resolve application version resources	Write	application* (p. 1504)		cloudformation:DescribeStacks cloudformation>ListStacks resource-groups:ListGroupResources resource-groups:DescribeGroup servicecatalog:DescribeOfferings servicecatalog:ListAssociations
StartAppAssessment	Grants permission to create application assessment	Write	application* (p. 1504)		cloudformation:DescribeStacks cloudformation>ListStacks cloudwatch:DescribeAlarms cloudwatch:GetMetricData cloudwatch:PutMetricData fis:GetExperimentTemplate fis>ListExperimentTemplate fis:ListExperiments resource-groups:ListGroupResources resource-groups:DescribeGroup servicecatalog:DescribeOfferings servicecatalog:ListAssociations ssm:GetParametersByPath

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 1504) aws:TagKeys (p. 1504)	
TagResource	Grants permission to assign a resource tag	Tagging	app-assessment (p. 1504) application (p. 1504) recommendation-template (p. 1504) resiliency-policy (p. 1503)		
UntagResource	Grants permission to untag a resource	Tagging	app-assessment (p. 1504) application (p. 1504) recommendation-template (p. 1504) resiliency-policy (p. 1503)		aws:TagKeys (p. 1504)
UpdateApp	Grants permission to update application	Write	application* (p. 1504)		
UpdateResiliencyPolicy	Grants permission to update Resiliency policy	Write	resiliency-policy* (p. 1503)		

Resource types defined by AWS Resilience Hub 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 \(p. 1499\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1504)

Resource types	ARN	Condition keys
application	arn:\${Partition}:resiliencehub:\${Region}: \${Account}:app/\${AppID}	aws:ResourceTag/ \${TagKey} (p. 1504)
app-assessment	arn:\${Partition}:resiliencehub:\${Region}: \${Account}:app-assessment/\${AppAssessmentID}	aws:ResourceTag/ \${TagKey} (p. 1504)
recommendation-template	arn:\${Partition}:resiliencehub:\${Region}: \${Account}:recommendation-template/ \${RecommendationTemplateID}	aws:ResourceTag/ \${TagKey} (p. 1504)

Condition keys for AWS Resilience Hub Service

AWS Resilience Hub 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 [Available global condition 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

AWS Resource Access Manager (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 \(p. 1505\)](#)
- [Resource types defined by AWS Resource Access Manager \(p. 1508\)](#)
- [Condition keys for AWS Resource Access Manager \(p. 1509\)](#)

Actions defined by AWS Resource 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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1508)		
					ram:ShareOwnerAccountId (p. 1509)
AssociateResourceSharePermissions	Grants permission to associate resource(s) and/or principal(s) to a resource share	Write	resource-share* (p. 1508)		
					aws:ResourceTag/\${TagKey} (p. 1509)
					ram:ResourceShareName (p. 1509)
					ram:AllowsExternalPrincipals (p. 1509)
					ram:Principal (p. 1509)
					ram:RequestedResourceType (p. 1509)
AssociateResourceSharePermissionsWith	Grants permission to associate permissions with a Resource Share	Write	permission* (p. 1508)		
			resource-share* (p. 1508)		
CreateResourceShare	Grants permission to create a resource share with provided resource(s) and/or principal(s)	Write			aws:RequestTags/CreateTags \${TagKey} (p. 1509) aws:TagKeys (p. 1509) ram:RequestedResourceType (p. 1509) ram:ResourceArn (p. 1509) ram:RequestedAllowsExternalPrincipal

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ram:Principal (p. 1509)	
DeleteResourceShare	Grants permission to delete a resource share	Write	resource-share* (p. 1508)		
				aws:ResourceTag/\${TagKey} (p. 1509) ram:ResourceShareName (p. 1509) ram:AllowsExternalPrincipals (p. 1509)	
DisassociateResourceShare	Grants permission to disassociate resource(s) and/or principal(s) from a resource share	Write	resource-share* (p. 1508)		
				aws:ResourceTag/\${TagKey} (p. 1509) ram:ResourceShareName (p. 1509) ram:AllowsExternalPrincipals (p. 1509) ram:Principal (p. 1509) ram:RequestedResourceType (p. 1509) ram:ResourceArn (p. 1509)	
DisassociateResourceSharePermission	Grants permission to disassociate a permission from a Resource Share	Write	permission* (p. 1508) resource-share* (p. 1508)		
EnableSharingWithCustomerOrganization	Grants permission to access a customer's organization and create a SLR in the customer's account	Permissions management			iam>CreateServiceLinkedRole (p. 1509) organizations:DescribeOrganizations (p. 1509) organizations:EnableAWSOrganizationsFeature (p. 1509)
GetPermission	Grants permission to get the contents of an AWS RAM permission	Read	permission* (p. 1508) ram:PermissionArn (p. 1509)		
GetResourcePolicy	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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetResourceShares	Grants permission to get a set of resource shares from a provided list or with a specified status	Read		aws:RequestTag/ \${TagKey} (p. 1509) aws:TagKeys (p. 1509)	
ListPendingInvitations	Grants permission to list the resource share that is shared with you but that the invitation is still pending for	Read	resource-share-invitation* (p. 1508)		
ListPermissionVersions	Grants permission to list the versions of an AWS RAM permission	List			
ListPermissions	Grants permission to list the AWS RAM permissions	List			
ListPrincipals	Grants permission to list the principals that you have shared resources with or that have shared resources with you	List			
ListResourceShares	Grants permission to list the permissions associated with a Resource Share	List	resource-share* (p. 1508)		
				aws:ResourceTag/ \${TagKey} (p. 1509)	ram:ResourceShareName (p. 1509) ram:AllowsExternalPrincipals (p. 1509)
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			
PromoteResourceShare	Grants permission to promote the specified resource share	Write	resource-share* (p. 1508)		
RejectResourceShare	Grants permission to reject the specified resource share invitation	Write	resource-share-invitation* (p. 1508)		
				ram:ShareOwnerAccountId (p. 1509)	
TagResource	Grants permission to tag the specified resource share	Tagging	resource-share* (p. 1508)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 1509) aws:TagKeys (p. 1509)	
UntagResource	Grants permission to untag the specified resource share	Tagging	resource-share* (p. 1508)		
				aws:RequestTag/ \${TagKey} (p. 1509) aws:TagKeys (p. 1509)	
UpdateResourceShare	Grants permission to update attributes of the resource share	Write	resource-share* (p. 1508)		
				aws:ResourceTag/ \${TagKey} (p. 1509) ram:ResourceShareName (p. 1509) ram:AllowsExternalPrincipals (p. 1509) ram:RequestedAllowsExternalPrincipals (p. 1509)	

Resource types defined by AWS Resource 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 \(p. 1505\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1509) ram:AllowsExternalPrincipals (p. 1509) ram:ResourceShareName (p. 1509)
resource-share-invitation	arn:\${Partition}:ram:\${Region}: \${Account}:resource-share-invitation/ \${ResourcePath}	ram:ShareOwnerAccountId (p. 1509)
permission	arn:\${Partition}:ram::\${Account}:permission/ \${ResourcePath}	ram:PermissionArn (p. 1509) ram:PermissionResourceType (p. 1509)

Condition keys for AWS Resource Access Manager

AWS Resource 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 [Available global condition keys](#).

Condition keys	Description	Type
aws:RequestTag/\${TagKey}	Filters access based on 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 based on the tags associated with the resource	String
aws:TagKeys	Filters access based on the tag keys that are passed when creating or tagging a resource share	ArrayOfString
ram:AllowsExternalPrincipals	Filters access based on 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 based on the specified Permission ARN	ARN
ram:PermissionResourceType	Filters access based on permissions of specified resource type	String
ram:Principal	Filters access based on the format of the specified principal	String
ram:RequestedAllowExternalPrincipals	Filters access based on the specified value for 'AllowExternalPrincipals'. External principals are AWS accounts that are outside of its AWS Organization	Bool
ram:RequestedResourceType	Filters access based on the specified resource type	String
ram:ResourceArn	Filters access based on a resource with the specified ARN	ARN
ram:ResourceShareName	Filters access based on a resource share with the specified name	String
ram:ShareOwnerAccount	Filters access based on resource shares owned by a specific account. For example, you can use this condition key to specify which resource share invitations can be accepted or rejected based on the resource share owner's account ID	String

Actions, resources, and condition keys for Amazon Resource Group Tagging API

Amazon Resource Group Tagging API (service prefix: tag) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

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

Topics

- [Actions defined by Amazon Resource Group Tagging API \(p. 1510\)](#)
- [Resource types defined by Amazon Resource Group Tagging API \(p. 1511\)](#)
- [Condition keys for Amazon Resource Group Tagging API \(p. 1511\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 <code>describe</code> the status of the <code>StartReportCreation</code> operation	Read			
GetComplianceSummary	Grants permission to retrieve a <code>summary</code> 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 key that	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	are used in the specified AWS Region for the calling account				
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 [Available keys for conditions](#).

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 \(p. 1512\)](#)
- [Resource types defined by AWS Resource Groups \(p. 1513\)](#)
- [Condition keys for AWS Resource Groups \(p. 1514\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateGroup	Grants permission to create a resource group with a specified name, description, and resource query	Write		aws:RequestTag/\${TagKey} (p. 1514) aws:TagKeys (p. 1514)	
DeleteGroup	Grants permission to delete a specified resource group	Write	group* (p. 1513)		
GetGroup	Grants permission to get information of a specified resource group	Read	group* (p. 1513)		
GetGroupConfig	Grants permission to get the service configuration associated with the specified resource group	Read	group* (p. 1513)		
GetGroupQuery	Grants permission to get the query associated with a specified resource group	Read	group* (p. 1513)		
GetTags	Grants permission to get the tags associated with a specified resource group	Read	group* (p. 1513)		
GroupResources	Grants permission to add the specified resources to the specified group	Write	group* (p. 1513)		
ListGroupResources	Grants permission to list the resources that are members of a specified resource group	List	group* (p. 1513)		cloudformation:DescribeStacks cloudformation>ListStacks tag:GetResources
ListGroups	Grants permission to list all resource groups in your account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutGroupConfigurations	Grants permission to put the service configuration associated with the specified resource group	Write	group* (p. 1513)		
PutGroupPolicy [permission only]	Grants permission to add a resource-based policy for the specified group	Write	group* (p. 1513)		
SearchResources	Grants permission to search for AWS resources matching the given query	List			cloudformation:DescribeStacks cloudformation>ListStacks tag:GetResources
Tag	Grants permission to tag a specified resource group	Tagging	group* (p. 1513)		
				aws:RequestTag/\${TagKey} (p. 1514)	
UngroupResources	Grants permission to remove the specified resources from the specified group	Write	group* (p. 1513)		
Untag	Grants permission to remove tags associated with a specified resource group	Tagging	group* (p. 1513)		
	aws:TagKeys (p. 1514)				
UpdateGroup	Grants permission to update a specified resource group	Write	group* (p. 1513)		
UpdateGroupQuery	Grants permission to update the query associated with a specified resource group	Write	group* (p. 1513)		

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 \(p. 1512\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
group	<code>arn:\${Partition}:resource-groups:\${Region}:\${Account}:group/\${GroupName}</code>	aws:ResourceTag/\${TagKey} (p. 1514)

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 [Available global condition 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 \(p. 1514\)](#)
- [Resource types defined by Amazon RHEL Knowledgebase Portal \(p. 1515\)](#)
- [Condition keys for Amazon RHEL Knowledgebase Portal \(p. 1515\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 [Available keys for conditions](#).

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 \(p. 1515\)](#)
- [Resource types defined by AWS RoboMaker \(p. 1520\)](#)
- [Condition keys for AWS RoboMaker \(p. 1521\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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			
BatchDescribeSimulationJobs	Describe multiple simulation jobs	Read			
CancelDeploymentJob	Cancel a deployment job	Write	deploymentJob* (p. 1521)		
CancelSimulationJob	Cancel a simulation job	Write	simulationJob* (p. 1521)		
CancelSimulationJobBatch	Cancel a simulation job batch	Write	simulationJobBatch* (p. 1521)		
CancelWorldExportJob	Cancel a world export job	Write	worldExportJob* (p. 1521)		
CancelWorldGenerationJob	Cancel a world generation job	Write	worldGenerationJob* (p. 1521)		
CreateDeploymentJob	Create a deployment job	Write		aws:TagKeys (p. 1522) aws:RequestTag/\${TagKey} (p. 1521)	CreateServiceLinkedRole
CreateFleet	Create a deployment fleet that represents a logical group of robots running the same robot application	Write		aws:TagKeys (p. 1522) aws:RequestTag/\${TagKey} (p. 1521)	CreateServiceLinkedRole
CreateRobot	Create a robot that can be registered to a fleet	Write		aws:TagKeys (p. 1522) aws:RequestTag/\${TagKey} (p. 1521)	CreateServiceLinkedRole
CreateRobotApplication	Create a robot application	Write		aws:TagKeys (p. 1522) aws:RequestTag/\${TagKey} (p. 1521)	
CreateRobotApplicationSnapshot	Create a snapshot of a robot application	Write	robotApplication* (p. 1521)	GetObject	
CreateSimulationApplication	Create a simulation application	Write		aws:TagKeys (p. 1522) aws:RequestTag/\${TagKey} (p. 1521)	
CreateSimulationApplicationSnapshot	Create a snapshot of a simulation application	Write	simulationApplication* (p. 1521)	GetObject	

Service Authorization Reference
Service Authorization Reference
AWS RoboMaker

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSimulationJob	Create a simulation job	Write		aws:TagKeys (p. 1522) aws:RequestTag/ \${TagKey} (p. 1521)	aws:CreateServiceLinkedRole (p. 1522)
CreateWorldExportJob	Create a world export job	Write	world* (p. 1521)		
				aws:TagKeys (p. 1522) aws:RequestTag/ \${TagKey} (p. 1521)	
CreateWorldGenerationJob	Create a world generation job	Write	worldTemplate* (p. 1521)		
				aws:TagKeys (p. 1522) aws:RequestTag/ \${TagKey} (p. 1521)	
CreateWorldTemplate	Create a world template	Write		aws:TagKeys (p. 1522) aws:RequestTag/ \${TagKey} (p. 1521)	
DeleteFleet	Delete a deployment fleet	Write		deploymentFleet* (p. 1521)	
DeleteRobot	Delete a robot	Write		robot* (p. 1521)	
DeleteRobotApplication	Delete a robot application	Write		robotApplication* (p. 1521)	
DeleteSimulationApplication	Delete a simulation application	Write		simulationApplication* (p. 1521)	
DeleteWorldTemplate	Delete a world template	Write		worldTemplate* (p. 1521)	
DeregisterRobot	Deregister a robot from a fleet	Write	deploymentFleet* (p. 1521)		
				robot* (p. 1521)	
DescribeDeploymentJob	Describe a deployment job	Read		deploymentJob* (p. 1521)	
DescribeFleet	Describe a deployment fleet	Read		deploymentFleet* (p. 1521)	
DescribeRobot	Describe a robot	Read		robot* (p. 1521)	
DescribeRobotApplication	Describe a robot application	Read		robotApplication* (p. 1521)	
DescribeSimulationApplication	Describe a simulation application	Read		simulationApplication* (p. 1521)	
DescribeSimulationJob	Describe a simulation job	Read		simulationJob* (p. 1521)	

Service Authorization Reference
Service Authorization Reference
AWS RoboMaker

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeSimulationJobBatch	Describe a simulation job batch	Read	simulationJobBatch* (p. 1521)		
DescribeWorld	Describe a world	Read	world* (p. 1521)		
DescribeWorldExportJob	Describe a world export job	Read	worldExportJob* (p. 1521)		
DescribeWorldGenerationJob	Describe a world generation job	Read	worldGenerationJob* (p. 1521)		
DescribeWorldTemplate	Describe a world template	Read	worldTemplate* (p. 1521)		
GetWorldTemplateBody	Get the body of a world template	Read	worldTemplate* (p. 1521)		
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			
ListSupportedAvailabilityZones [permission only]	Lists supported availability zones	List			
ListTagsForResource	List tags for a RoboMaker resource	List	deploymentFleet (p. 1521) deploymentJob (p. 1521) robot (p. 1521) robotApplication (p. 1521) simulationApplication (p. 1521) simulationJob (p. 1521) simulationJobBatch (p. 1521) world (p. 1521)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			worldExportJob (p. 1521)		
			worldGenerationJob (p. 1521)		
			worldTemplate (p. 1521)		
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* (p. 1521)		
			robot* (p. 1521)		
RestartSimulationJob	Restart a running simulation job	Write	simulationJob* (p. 1521)		
StartSimulationJobBatch	Create a simulation job batch	Write	aws:TagKeys (p. 1521) aws:RequestTag/\${TagKey} (p. 1521)	iam:CreateServiceLinkedRole (p. 1521)	
SyncDeploymentJobs	Ensures the most recently deployed robot application is deployed to all robots in the fleet	Write			
TagResource	Add tags to a RoboMaker resource	Tagging	deploymentFleet (p. 1521)		
			deploymentJob (p. 1521)		
			robot (p. 1521)		
			robotApplication (p. 1521)		
			simulationApplication (p. 1521)		
			simulationJob (p. 1521)		
			simulationJobBatch (p. 1521)		
			world (p. 1521)		
			worldExportJob (p. 1521)		
			worldGenerationJob (p. 1521)		
			worldTemplate (p. 1521)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys (p. 1522) aws:RequestTag/ \${TagKey} (p. 1521)	
UntagResource	Remove tags from a RoboMaker resource	Tagging	deploymentFleet (p. 1521) deploymentJob (p. 1521) robot (p. 1521) robotApplication (p. 1521) simulationApplication (p. 1521) simulationJob (p. 1521) simulationJobBatch (p. 1521) world (p. 1521) worldExportJob (p. 1521) worldGenerationJob (p. 1521) worldTemplate (p. 1521)		aws:TagKeys (p. 1522)
UpdateRobotApplication	Update a robot application	Write	robotApplication* (p. 1521)		
UpdateRobotDeployment [permission only]	Report the deployment status for an individual robot	Write			
UpdateSimulationApplication	Update a simulation application	Write	simulationApplication* (p. 1521)		
UpdateWorldTemplate	Update a world template	Write	worldTemplate* (p. 1521)		

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 \(p. 1515\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1522)
simulationApplication	arn:\${Partition}:robomaker:\${Region}: \${Account}:simulation-application/ \${ApplicationName}/\${CreatedOnEpoch}	aws:ResourceTag/ \${TagKey} (p. 1522)
simulationJob	arn:\${Partition}:robomaker:\${Region}: \${Account}:simulation-job/\${SimulationJobId}	aws:ResourceTag/ \${TagKey} (p. 1522)
simulationJobBatch	arn:\${Partition}:robomaker:\${Region}: \${Account}:simulation-job-batch/ \${SimulationJobBatchId}	aws:ResourceTag/ \${TagKey} (p. 1522)
deploymentJob	arn:\${Partition}:robomaker:\${Region}: \${Account}:deployment-job/\${DeploymentJobId}	aws:ResourceTag/ \${TagKey} (p. 1522)
robot	arn:\${Partition}:robomaker:\${Region}: \${Account}:robot/\${RobotName}/ \${CreatedOnEpoch}	aws:ResourceTag/ \${TagKey} (p. 1522)
deploymentFleet	arn:\${Partition}:robomaker:\${Region}: \${Account}:deployment-fleet/\${FleetName}/ \${CreatedOnEpoch}	aws:ResourceTag/ \${TagKey} (p. 1522)
worldGenerationJob	arn:\${Partition}:robomaker:\${Region}: \${Account}:world-generation-job/ \${WorldGenerationJobId}	aws:ResourceTag/ \${TagKey} (p. 1522)
worldExportJob	arn:\${Partition}:robomaker:\${Region}: \${Account}:world-export-job/ \${WorldExportJobId}	aws:ResourceTag/ \${TagKey} (p. 1522)
worldTemplate	arn:\${Partition}:robomaker: \${Region}: \${Account}:world-template/ \${WorldTemplateJobId}	aws:ResourceTag/ \${TagKey} (p. 1522)
world	arn:\${Partition}:robomaker:\${Region}: \${Account}:world/\${WorldId}	aws:ResourceTag/ \${TagKey} (p. 1522)

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 [Available global condition 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 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 \(p. 1522\)](#)
- [Resource types defined by Amazon Route 53 \(p. 1528\)](#)
- [Condition keys for Amazon Route 53 \(p. 1529\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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*	(p. 1529)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateVPCWithHostedZone	Grants permission to associate an additional Amazon VPC with a private hosted zone	Write	hostedzone (p. 1529)		ec2:DescribeVpcs
ChangeResourceRecordSets	Grants permission to create, update or delete a record, which contains authoritative DNS information for a specified domain or subdomain name	Write	hostedzone* (p. 1529)		
ChangeTagsForHealthCheck	Grants permission to add, edit, or delete tags for a health check or a hosted zone	Tagging	healthcheck* (p. 1529)		
CreateTagsForHostedZone			hostedzone* (p. 1529)		
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			ec2:DescribeVpcs
CreateKeySigningKey	Grants permission to create a key-signing key associated with a hosted zone	Write	hostedzone* (p. 1529)		
CreateQueryLoggingConfiguration	Grants permission to create a configuration for DNS query logging	Write	hostedzone* (p. 1529)		
CreateReusableDelegationSet	Grants permission to create a delegation set (a group of four name servers) that can be reused by multiple hosted zones	Write			
CreateTrafficPolicy	Grants permission to create a traffic policy, which you use to create multiple DNS records for one domain name (such as example.com) or one subdomain name (such as www.example.com)	Write			
CreateTrafficPolicyRecords	Grants permission to create records in a specified hosted zone based on the settings in a specified traffic policy version	Write	hostedzone* (p. 1529)		
			trafficpolicy* (p. 1529)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTrafficPolicy	Grants permission to create a new version of an existing traffic policy	Write	trafficpolicy* (p. 1529)		
CreateVPCAssociationAuthorization	Grants permission to authorize another AWS account that created a specified VPC to submit an AssociateVPCWithHostedZone request, which associates the VPC with a specified hosted zone that was created by a different account	Write	hostedzone* (p. 1529)		
DeactivateKeySigningKey	Grants permission to deactivate a key-signing key so that it will not be used for signing by DNSSEC	Write	hostedzone* (p. 1529)		
DeleteHealthCheck	Grants permission to delete a health check	Write	healthcheck* (p. 1529)		
DeleteHostedZone	Grants permission to delete a hosted zone	Write	hostedzone* (p. 1529)		
DeleteKeySigningKey	Grants permission to delete a key-signing key	Write	hostedzone* (p. 1529)		
DeleteQueryLoggingConfiguration	Grants permission to delete a configuration for DNS query logging	Write	queryloggingconfig* (p. 1529)		
DeleteReusableDelegationSet	Grants permission to delete a reusable delegation set	Write	delegationset* (p. 1529)		
DeleteTrafficPolicy	Grants permission to delete a traffic policy	Write	trafficpolicy* (p. 1529)		
DeleteTrafficPolicyInstance	Grants permission to delete a traffic policy instance and all the records that Route 53 created when you created the instance	Write	trafficpolicyinstance* (p. 1529)		
DeleteVPCAssociationAuthorization	Grants permission to remove authorization for associating an Amazon Virtual Private Cloud with a Route 53 private hosted zone	Write	hostedzone* (p. 1529)		
DisableHostedZoneDNSSEC	Grants permission to disable DNSSEC signing in a specific hosted zone	Write	hostedzone* (p. 1529)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateVPC	Grants permission to disassociate one Amazon Virtual Private Cloud from a Route 53 private hosted zone	Write	hostedzone (p. 1529)		ec2:DescribeVpcs
EnableHostedZoneDNSSEC	Grants permission to enable DNSSEC signing in a specific hosted zone	Write	hostedzone* (p. 1529)		
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* (p. 1529)		
GetCheckerIpRanges	Grants permission to get a list of the IP ranges that are used by Route 53 health checkers to check the health of your resources	List			
GetDNSSEC	Grants permission to get information about DNSSEC for a specific hosted zone, including the key-signing keys in the hosted zone	Read	hostedzone* (p. 1529)		
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* (p. 1529)		
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* (p. 1529)		
GetHealthCheckStatus	Grants permission to get the status of a specified health check	List	healthcheck* (p. 1529)		

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* (p. 1529)		
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* (p. 1529)		
GetQueryLoggingConfiguration	Grants permission to get information about a specified configuration for DNS query logging	Read	queryloggingconfig* (p. 1529)		
GetReusableDelegationSetInformation	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* (p. 1529)		
GetReusableDelegationSetSummary	Grants permission to get the maximum number of hosted zones that you can associate with the specified reusable delegation set	Read	delegationset* (p. 1529)		
GetTrafficPolicy	Grants permission to get information about a specified traffic policy version	Read	trafficpolicy* (p. 1529)		
GetTrafficPolicyInstanceInformation	Grants permission to get information about a specified traffic policy instance	Read	trafficpolicyinstance* (p. 1529)		
GetTrafficPolicyInstancesInMemberAccount	Grants permission to get the number of traffic policy instances that are associated with the current AWS account	Read			
ListGeoLocations	Grants permission to get a list of geographic locations that Route 53 supports for geolocation	Read			
ListHealthChecks	Grants permission to get a list of the health checks that are associated with the current AWS account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListHostedZones	Grants permission to get a list of the public and private hosted zones that are associated with the current AWS account	List			
ListHostedZonesByQueryConfigurations	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 the private hosted zones that a specified VPC is associated with	List			ec2:DescribeVpcs
ListQueryLoggingConfigurations	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 (p. 1529)		
ListResourceRecords	Grants permission to list the records in a specified hosted zone	List	hostedzone* (p. 1529)		
ListReusableDelegationSets	Grants permission to list the 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 (p. 1529)		
			hostedzone (p. 1529)		
ListTagsForResources	Grants permission to list tags for up to 10 health checks or hosted zones	Read	healthcheck (p. 1529)		
			hostedzone (p. 1529)		
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			
ListTrafficPolicyInformation	Grants permission to get information about the traffic policy instances that you created by using the current AWS account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTrafficPolicyInformation	Grants permission to get information about the traffic policy instances that you created in a specified hosted zone	List	hostedzone* (p. 1529)		
ListTrafficPolicyInformation	Grants permission to get information about the traffic policy instances that you created using a specified traffic policy version	List	trafficpolicy* (p. 1529)		
ListTrafficPolicyVersions	Grants permission to get information about all the versions for a specified traffic policy	List	trafficpolicy* (p. 1529)		
ListVPCAssociations	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* (p. 1529)		
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* (p. 1529)		
UpdateHostedZoneComment	Grants permission to update the comment for a specified hosted zone	Write	hostedzone* (p. 1529)		
UpdateTrafficPolicyComment	Grants permission to update the comment for a specified traffic policy version	Write	trafficpolicy* (p. 1529)		
UpdateTrafficPolicyRecords	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* (p. 1529)		

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 \(p. 1522\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
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

Route 53 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 [Available keys for conditions](#).

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 \(p. 1529\)](#)
- [Resource types defined by Amazon Route 53 Domains \(p. 1532\)](#)
- [Condition keys for Amazon Route 53 Domains \(p. 1533\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptDomainTransfer	Grants permission to accept the transfer of a domain from another AWS account to the current AWS account	Write			
CancelDomainTransfer	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			
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			
EnableDomainAutoRenew	Grants permission to configure Amazon Route 53 to automatically renew the specified domain before the domain registration expires	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableDomainTransfer	Grants permission to set the transfer lock on the domain (specifically the clientTransferProhibited status) to prevent domain transfers	Write			
GetContactReachabilityInformation	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			
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			
RegisterDomain	Grants permission to register domains	Write			
RejectDomainTransfer	Grants permission to reject the transfer of a domain from another AWS account to the current AWS account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RenewDomain	Grants permission to renew domains for the specified number of years	Write			
ResendContactReactivationEmail	Grants permission to resend the activation 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			
RetrieveDomainAuthCode	Grants permission to get the Auth Code for the domain	Write			
TransferDomain	Grants permission to transfer a domain from another registrar to Amazon Route 53	Write			
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			
UpdateDomainContactPrivacySetting	Grants permission to update the domain privacy contact 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 [Available keys for conditions](#).

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 \(p. 1533\)](#)
- [Resource types defined by Amazon Route 53 Recovery Cluster \(p. 1534\)](#)
- [Condition keys for Amazon Route 53 Recovery Cluster \(p. 1534\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRoutingControls	Grants permission to get a routing control state	Read	routingcontrol* (p. 1534)		
ListRoutingControls	Grants permission to list routing controls	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateRoutingControlConfig	Grants permission to update a routing control state	Write	routingcontrol* (p. 1534)		
				route53-recovery-cluster:AllowSafetyRulesOverrides (p. 1534)	
UpdateRoutingControlStates	Grants permission to update a routing control states	Write	routingcontrol* (p. 1534)		
				route53-recovery-cluster:AllowSafetyRulesOverrides (p. 1534)	

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 \(p. 1533\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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 [Available global condition 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 \(p. 1535\)](#)
- [Resource types defined by Amazon Route 53 Recovery Controls \(p. 1537\)](#)
- [Condition keys for Amazon Route 53 Recovery Controls \(p. 1537\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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	cluster* (p. 1537)		
				aws:RequestTag/\${TagKey} (p. 1538)	
				aws:TagKeys (p. 1538)	
CreateControlPanel	Grants permission to create a control panel	Write	controlpanel* (p. 1537)		
				aws:RequestTag/\${TagKey} (p. 1538)	
				aws:TagKeys (p. 1538)	
CreateRoutingControl	Grants permission to create a routing control	Write	routingcontrol* (p. 1537)		
CreateSafetyRule	Grants permission to create a safety rule	Write	safetyrule* (p. 1537)		
				aws:RequestTag/\${TagKey} (p. 1538)	
				aws:TagKeys (p. 1538)	

Service Authorization Reference
Service Authorization Reference
Amazon Route 53 Recovery Controls

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteCluster	Grants permission to delete a cluster	Write	cluster* (p. 1537)		
DeleteControlPanel	Grants permission to delete a control panel	Write	controlpanel* (p. 1537)		
DeleteRoutingControl	Grants permission to delete a routing control	Write	routingcontrol* (p. 1537)		
DeleteSafetyRule	Grants permission to delete a safety rule	Write	safetyrule* (p. 1537)		
DescribeCluster	Grants permission to describe a cluster	Read	cluster* (p. 1537)		
DescribeControlPanel	Grants permission to describe a control panel	Read	controlpanel* (p. 1537)		
DescribeRoutingControl	Grants permission to describe a routing control	Read	routingcontrol* (p. 1537)		
DescribeRoutingControlByControl	Grants permission to describe a routing control	Read	routingcontrol* (p. 1537)		
DescribeSafetyRule	Grants permission to describe a safety rule	Read	safetyrule* (p. 1537)		
ListAssociatedRoute53HealthChecks	Grants permission to list associated Route 53 health checks	List			
ListClusters	Grants permission to list clusters	Read			
ListControlPanels	Grants permission to list control panels	Read			
ListRoutingControls	Grants permission to list routing controls	Read			
ListSafetyRules	Grants permission to list safety rules	Read	controlpanel* (p. 1537)		
ListTagsForResource	Grants permission to list tags for a resource	Read			
TagResource	Grants permission to tag a resource	Tagging	cluster (p. 1537)		
			controlpanel (p. 1537)		
			safetyrule (p. 1537)		
				aws:TagKeys (p. 1538)	
				aws:RequestTag/\${TagKey} (p. 1538)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagResource	Grants permission to remove tags from a resource	Tagging	cluster (p. 1537) controlpanel (p. 1537) safetyrule (p. 1537)		
			aws:TagKeys (p. 1538) aws:RequestTag/\${TagKey} (p. 1538)		
UpdateControlPanel	Grants permission to update a cluster	Write	controlpanel* (p. 1537)		
UpdateRoutingControl	Grants permission to update a routing control	Write	routingcontrol* (p. 1537)		
UpdateSafetyRule	Grants permission to update a safety rule	Write	safetyrule* (p. 1537)		

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 \(p. 1535\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1538)
controlpanel	arn:\${Partition}:route53-recovery-control::\${Account}:controlpanel/\${ControlPanelId}	aws:ResourceTag/\${TagKey} (p. 1538)
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} (p. 1538)

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 [Available global condition keys](#).

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

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 \(p. 1538\)](#)
- [Resource types defined by Amazon Route 53 Recovery Readiness \(p. 1541\)](#)
- [Condition keys for Amazon Route 53 Recovery Readiness \(p. 1542\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1541)		
				aws:RequestTag/ \${TagKey} (p. 1542)	
				aws:TagKeys (p. 1542)	
CreateCrossAccountAuthorization	Grants permission to create a cross-account authorization	Write			
CreateReadinessCheck	Grants permission to create a readiness check	Write	readinesscheck* (p. 1541)		
				aws:RequestTag/ \${TagKey} (p. 1542)	
				aws:TagKeys (p. 1542)	
CreateRecoveryGroup	Grants permission to create a recovery group	Write	recoverygroup* (p. 1542)		
				aws:RequestTag/ \${TagKey} (p. 1542)	
				aws:TagKeys (p. 1542)	
CreateResourceSet	Grants permission to create a resource set	Write	resourceset* (p. 1541)		
				aws:RequestTag/ \${TagKey} (p. 1542)	
				aws:TagKeys (p. 1542)	
DeleteCell	Grants permission to delete a cell	Write	cell* (p. 1541)		
DeleteCrossAccountAuthorization	Grants permission to delete a cross-account authorization	Write			
DeleteReadinessCheck	Grants permission to delete a readiness check	Write	readinesscheck* (p. 1541)		
DeleteRecoveryGroup	Grants permission to delete a recovery group	Write	recoverygroup* (p. 1542)		
DeleteResourceSet	Grants permission to delete a resource set	Write	resourceset* (p. 1541)		
GetArchitectureRecommendations	Grants permission to get architecture recommendations for a recovery group	Read	recoverygroup* (p. 1542)		
GetCell	Grants permission to get information about a cell	Read	cell* (p. 1541)		
GetCellReadinessSummary	Grants permission to get a readiness summary for a cell	Read	cell* (p. 1541)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetReadinessCheck	Grants permission to get information about a readiness check	Read	readinesscheck* (p. 1541)		
GetReadinessCheckStatus	Grants permission to get the readiness status for an individual resource	Read	readinesscheck* (p. 1541)		
GetReadinessCheckStatusOf	Grants permission to get the status of a readiness check (for a resource set)	Read	readinesscheck* (p. 1541)		
GetRecoveryGroup	Grants permission to get information about a recovery group	Read	recoverygroup* (p. 1542)		
GetRecoveryGroupReadinessSummary	Grants permission to get ReadinessSummary for a recovery group	Read	recoverygroup* (p. 1542)		
GetResourceSet	Grants permission to get information about a resource set	Read	resourceset* (p. 1541)		
ListCells	Grants permission to list cells	Read			
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			
ListTagsForResource	Grants permission to list tags for a resource	Read			
TagResource	Grants permission to add a tag to a resource	Tagging	cell (p. 1541)		
			readinesscheck (p. 1541)		
			recoverygroup (p. 1542)		
			resourceset (p. 1541)		
			aws:TagKeys (p. 1542) aws:RequestTag/ {\$TagKey} (p. 1542)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagResource	Grants permission to remove a tag from a resource	Tagging	cell (p. 1541) readinesscheck (p. 1541) recoverygroup (p. 1542) resourceset (p. 1541)		
				aws:TagKeys (p. 1542) aws:RequestTag/ \${TagKey} (p. 1542)	
				cell* (p. 1541) aws:TagKeys (p. 1542)	
				readinesscheck* (p. 1541) aws:TagKeys (p. 1542)	
				recoverygroup* (p. 1542) aws:TagKeys (p. 1542)	
UpdateCell	Grants permission to update a cell	Write			
UpdateReadinessCheck	Grants permission to update a readiness check	Write			
UpdateRecoveryGroup	Grants permission to update a recovery group	Write			
UpdateResourceSet	Grants permission to update a resource set	Write		resourceset* (p. 1541)	
					aws:TagKeys (p. 1542)

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 \(p. 1538\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1542)
resourceset	arn:\${Partition}:route53-recovery-readiness:::\${Account}:resource-set/\${ResourceId}	aws:ResourceTag/ \${TagKey} (p. 1542)
cell	arn:\${Partition}:route53-recovery-readiness:::\${Account}:cell/\${ResourceId}	aws:ResourceTag/ \${TagKey} (p. 1542)

Resource types	ARN	Condition keys
recoverygroup	arn:\${Partition}:route53-recovery-readiness::\${Account}:recovery-group/\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 1542)

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 [Available global condition 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	String

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 \(p. 1542\)](#)
- [Resource types defined by Amazon Route 53 Resolver \(p. 1550\)](#)
- [Condition keys for Amazon Route 53 Resolver \(p. 1551\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateFirewallRuleWithAmazonVPC	Grants permission to associate an Amazon VPC with a specified firewall rule group	Write	firewall-rule-group-association* (p. 1551)		ec2:DescribeVpcs
				aws:RequestTag/\${TagKey} (p. 1551) aws:TagKeys (p. 1551)	
AssociateResolverEndpointWithIPAddress	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* (p. 1551)		
AssociateResolverQueryLoggingConfig	Grants permission to associate an Amazon VPC with a specified query logging configuration	Write	resolver-query-log-config* (p. 1551)		
AssociateResolverRuleWithVPC	Grants permission to associate a specified Resolver rule with a specified VPC	Write	resolver-rule* (p. 1551)		
CreateFirewallDomainList	Grants permission to create a Firewall domain list	Write	firewall-domain-list* (p. 1551)		
				aws:RequestTag/\${TagKey} (p. 1551) aws:TagKeys (p. 1551)	
CreateFirewallRule	Grants permission to create a Firewall rule within a Firewall rule group	Write	firewall-rule-group* (p. 1551)		
CreateFirewallRuleGroup	Grants permission to create a Firewall rule group	Write	firewall-rule-group* (p. 1551)		
				aws:RequestTag/\${TagKey} (p. 1551)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					aws:TagKeys (p. 1551)
CreateResolverEndpoint	Grants permission to create a Resolver endpoint . There are two types of Resolver endpoints, inbound and outbound	Write	resolver-endpoint* (p. 1551)		
					aws:RequestTag/\${TagKey} (p. 1551) aws:TagKeys (p. 1551)
CreateResolverQueryLoggingConfig	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* (p. 1551)		
					aws:RequestTag/\${TagKey} (p. 1551) aws:TagKeys (p. 1551)
CreateResolverRule	Grants permission to define how to route queries originating from your VPC out of the VPC	Write	resolver-rule* (p. 1551)		
					aws:RequestTag/\${TagKey} (p. 1551) aws:TagKeys (p. 1551)
DeleteFirewallDomainList	Grants permission to delete a Firewall domain list	Write	firewall-domain-list* (p. 1551)		
DeleteFirewallRule	Grants permission to delete a Firewall rule within a Firewall rule group	Write	firewall-rule-group* (p. 1551)		
DeleteFirewallRuleGroup	Grants permission to delete a Firewall rule group	Write	firewall-rule-group* (p. 1551)		
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* (p. 1551)		
DeleteResolverQueryLoggingConfig	Grants permission to delete a Resolver query logging configuration	Write	resolver-query-log-config* (p. 1551)		
DeleteResolverRule	Grants permission to delete a Resolver rule	Write	resolver-rule* (p. 1551)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateFirewallRuleGroupAssociation	Grants permission to remove the association between a specified Firewall rule group and a specified VPC	Write	firewall-rule-group-association* (p. 1551)		
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* (p. 1551)		
DisassociateResolverQueryLogConfig	Grants permission to remove the association between a specified Resolver query logging configuration and a specified VPC	Write	resolver-query-log-config* (p. 1551)		
DisassociateResolverRule	Grants permission to remove the association between a specified Resolver rule and a specified VPC	Write	resolver-rule* (p. 1551)		
GetFirewallConfig	Grants permission to get information about a specified Firewall config	Read	firewall-config* (p. 1551)		ec2:DescribeVpcs
GetFirewallDomainList	Grants permission to get information about a specified Firewall domain list	Read	firewall-domain-list* (p. 1551)		
GetFirewallRuleGroup	Grants permission to get information about a specified Firewall rule group	Read	firewall-rule-group* (p. 1551)		
GetFirewallRuleGroupAssociation	Grants permission to get information about an association between a specified Firewall rule group and a VPC	Read	firewall-rule-group-association* (p. 1551)		
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* (p. 1551)		
GetResolverConfig	Grants permission to get the Resolver Config status within the specified resource	Read	resolver-config* (p. 1551)		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* (p. 1551)		
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* (p. 1551)		
GetResolverQueryLoggingConfiguration	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* (p. 1551)		
GetResolverQueryLoggingConfigurationAssociation	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	resolver-query-log-config* (p. 1551)		
GetResolverQueryLoggingPolicy	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* (p. 1551)		
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	resolver-rule* (p. 1551)		
GetResolverRuleAssociation	Grants permission to get information about an association between a specified Resolver rule and a VPC	Read	resolver-rule* (p. 1551)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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* (p. 1551)		
ImportFirewallDomains	Grants permission to add, remove or replace Firewall domains in a Firewall domain list	Write	firewall-domain-list* (p. 1551)		
ListFirewallConfigurations	Grants permission to list all the Firewall config that current AWS account is able to check	List	firewall-config* (p. 1551)		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* (p. 1551)		
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* (p. 1551)		
ListResolverConfigurations	Grants permission to list Resolver Config statuses	List	resolver-config* (p. 1551)		ec2:DescribeVpcs
ListResolverDnssecConfigurations	Grants permission to list the DNSSEC validation support status for DNS queries	List	resolver-dnssec-config* (p. 1551)		
ListResolverEndpointAddresses	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* (p. 1551)		
ListResolverEndpoints	Grants permission to list all the Resolver endpoints that were created using the current AWS account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListResolverQueryInformation	Grants permission to list information about associations between Amazon VPCs and query logging configurations	List	resolver-query-log-config* (p. 1551)		
ListResolverQueryLogConfigurations	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	resolver-query-log-config* (p. 1551)		
ListResolverRuleAssociations	Grants permission to list the associations that were created between Resolver rules and VPCs using the current AWS account	List			
ListResolverRules	Grants permission to list the Resolver rules that were created using the current AWS account	List			
ListTagsForResource	Grants permission to list the tags that you associated with the specified resource	Read	firewall-domain-list (p. 1551)		
firewall-rule-group (p. 1551)					
firewall-rule-group-association (p. 1551)					
resolver-endpoint (p. 1551)					
resolver-query-log-config (p. 1551)					
resolver-rule (p. 1551)					
PutFirewallRuleGroup	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* (p. 1551)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutResolverQueryLoggingConfiguration	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* (p. 1551)		
PutResolverRuleShare	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* (p. 1551)		
TagResource	Grants permission to add one or more tags to a specified resource	Tagging	firewall-domain-list (p. 1551)		
			firewall-rule-group (p. 1551)		
			firewall-rule-group-association (p. 1551)		
			resolver-endpoint (p. 1551)		
			resolver-query-log-config (p. 1551)		
			resolver-rule (p. 1551)		
UntagResource	Grants permission to remove one or more tags from a specified resource	Tagging	firewall-domain-list (p. 1551)		
			firewall-rule-group (p. 1551)		
			firewall-rule-group-association (p. 1551)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			resolver-endpoint (p. 1551)		
			resolver-query-log-config (p. 1551)		
			resolver-rule (p. 1551)		
UpdateFirewallConfig	Grants permission to update selected settings for an Firewall config	Write	firewall-config* (p. 1551)		ec2:DescribeVpcs
UpdateFirewallDomainList	Grants permission to add, remove or replace Firewall domains in a Firewall domain list	Write	firewall-domain-list* (p. 1551)		
UpdateFirewallRuleGroup	Grants permission to update selected settings for an Firewall rule in a Firewall rule group	Write	firewall-rule-group* (p. 1551)		
UpdateFirewallRuleGroupAssociation	Grants permission to update selected settings for an Firewall rule group association	Write	firewall-rule-group-association* (p. 1551)		
UpdateResolverConfig	Grants permission to update the Resolver Config status within the specified resource	Write	resolver-config* (p. 1551)		ec2:DescribeVpcs
UpdateResolverDnssecConfig	Grants permission to update the DNSSEC validation support status for DNS queries within the specified resource	Write	resolver-dnssec-config* (p. 1551)		
UpdateResolverEndpoint	Grants permission to update selected settings for an inbound or an outbound Resolver endpoint	Write	resolver-endpoint* (p. 1551)		
UpdateResolverRule	Grants permission to update settings for a specified Resolver rule	Write	resolver-rule* (p. 1551)		

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 \(p. 1542\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1551)
resolver-query-log-config	arn:\${Partition}:route53resolver:\${Region}: \${Account}:resolver-query-log-config/\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 1551)
resolver-rule	arn:\${Partition}:route53resolver:\${Region}: \${Account}:resolver-rule/\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 1551)
resolver-endpoint	arn:\${Partition}:route53resolver:\${Region}: \${Account}:resolver-endpoint/\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 1551)
firewall-rule-group	arn:\${Partition}:route53resolver:\${Region}: \${Account}:firewall-rule-group/\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 1551)
firewall-rule-group-association	arn:\${Partition}:route53resolver:\${Region}: \${Account}:firewall-rule-group-association/\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 1551)
firewall-domain-list	arn:\${Partition}:route53resolver: \${Region}: \${Account}:firewall-domain-list/\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 1551)
firewall-config	arn:\${Partition}:route53resolver:\${Region}: \${Account}:firewall-config/\${ResourceId}	aws:ResourceTag/\${TagKey} (p. 1551)
resolver-config	arn:\${Partition}:route53resolver:\${Region}: \${Account}:resolver-config/\${ResourceId}	

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 [Available global condition 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	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 \(p. 1552\)](#)
- [Resource types defined by Amazon S3 \(p. 1610\)](#)
- [Condition keys for Amazon S3 \(p. 1611\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1610) s3:DataAccessPointArn (p. 1611) s3:DataAccessPointAccount (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)		

Service Authorization Reference
Service Authorization Reference
Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	BypassGovernanceRetention	Permissions management	object* (p. 1610)		

Service Authorization Reference
 Service Authorization Reference
 Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to allow circumvention of governance-mode object retention settings			s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:RequestObjectTag/ <key> (p. 1611) s3:RequestObjectTagKeys (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-acl (p. 1612) s3:x-amz-content-sha256 (p. 1612) s3:x-amz-copy-source (p. 1612) s3:x-amz-grant-full-control (p. 1612) s3:x-amz-grant-read (p. 1612) s3:x-amz-grant-read-acp (p. 1612) s3:x-amz-grant-write (p. 1613) s3:x-amz-grant-write-acp (p. 1613)	

Service Authorization Reference
 Service Authorization Reference
 Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:x-amz-metadata-directive (p. 1613) s3:x-amz-server-side-encryption (p. 1613) s3:x-amz-server-side-encryption-aws-kms-key-id (p. 1613) s3:x-amz-storage-class (p. 1613) s3:x-amz-website-redirect-location (p. 1613) s3:object-lock-mode (p. 1612) s3:object-lock-retain-until-date (p. 1612) s3:object-lock-remaining-retention-days (p. 1612) s3:object-lock-legal-hold (p. 1612)	
CreateAccessPoint	Grants permission to create a new access point	Write	accesspoint* (p. 1610)		

Service Authorization Reference
 Service Authorization Reference
 Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:authType (p. 1612) s3:locationconstraint (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-acl (p. 1612) s3:x-amz-content-sha256 (p. 1612)
CreateAccessPoint	Grants permission to create an Object Lambda -enabled accesspoint	Write	objectlambdaaccesspoint* (p. 1610)		s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)
CreateBucket	Grants permission to create a new bucket	Write	bucket* (p. 1610)		

Service Authorization Reference
 Service Authorization Reference
 Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					s3:authType (p. 1612) s3:locationconstraint (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-acl (p. 1612) s3:x-amz-content-sha256 (p. 1612) s3:x-amz-grant-full-control (p. 1612) s3:x-amz-grant-read (p. 1612) s3:x-amz-grant-read-acp (p. 1612) s3:x-amz-grant-write (p. 1613) s3:x-amz-grant-write-acp (p. 1613) s3:x-amz-object-ownership (p. 1613)

Service Authorization Reference
Service Authorization Reference
Amazon S3

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 (iam:PassRole) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612) s3:RequestJobPriority (p. 1611) s3:RequestJobOperation (p. 1611) aws:TagKeys (p. 1611) aws:RequestTag/ \${TagKey} (p. 1611)
CreateMultiRegionAccessPoint	Grants permission to create a new multi-region access point	Write	multiregionaccesspoint* (p. 1610)		
					s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) aws:RequestedRegion (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureversion (p. 1612) s3:signatureAge (p. 1612) s3:TlsVersion (p. 1612)
DeleteAccessPoint	Grants permission to delete the access point named in the URI	Write	accesspoint* (p. 1610)		

Service Authorization Reference
Service Authorization Reference
Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					s3:DataAccessPointArn (p. 1611) s3:DataAccessPointAccount (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)
DeleteAccessPointObjectLambdaEnabled	Grants permission to delete the objectlambdaenabled access point named in the URI	Write	objectlambdaaccesspoint* (p. 1610)		s3:DataAccessPointArn (p. 1611) s3:DataAccessPointAccount (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)
DeleteAccessPointPolicy	Grants permission to delete the policy on a specified access point	Permissions management	accesspoint* (p. 1610)		

Service Authorization Reference
Service Authorization Reference
Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					s3:DataAccessPointArn (p. 1611) s3:DataAccessPointAccount (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)
DeleteAccessPoint	Grants permission to delete the policy object specified object lambda enabled access point	Permissions management	objectlambdaaccesspoint* (p. 1610)		s3:DataAccessPointArn (p. 1611) s3:DataAccessPointAccount (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)
DeleteBucket	Grants permission to delete the bucket named in the URI	Write	bucket* (p. 1610) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)		

Service Authorization Reference
Service Authorization Reference
Amazon S3

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* (p. 1610)	s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
DeleteBucketWebsite	Grants permission to remove the website configuration for a bucket	Write	bucket* (p. 1610)	s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
DeleteJobTagging	Grants permission to remove tags from an existing Amazon S3 Batch Operations job	Tagging	job* (p. 1610)	s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612) s3:ExistingJobPriority (p. 1611) s3:ExistingJobOperation (p. 1611)	
DeleteMultiRegionAccessPoint		Write	multiregionaccesspoint* (p. 1610)		

Service Authorization Reference
 Service Authorization Reference
 Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to delete the multi region access point named in the URI			s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) aws:RequestedRegion (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureversion (p. 1612) s3:signatureAge (p. 1612) s3:TlsVersion (p. 1612)	
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* (p. 1610)		
				s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	

Service Authorization Reference
Service Authorization Reference
Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteObjectTagging	Grants permission to use the <code>Tagging</code> subresource to remove the entire tag set from the specified object	Tagging	object* (p. 1610)		
DeleteObjectVersionTagging	Grants permission to remove a specific version of an object	Write	object* (p. 1610)		
		Tagging	object* (p. 1610)		

Service Authorization Reference
Service Authorization Reference
Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to remove the entire tag set for a specific version of the object			s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:ExistingObjectTag/ <key> (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:versionid (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
DeleteStorageLensConfiguration	Grants permission to delete an existing Amazon S3 Storage Lens configuration	Write	storagelensconfiguration* (p. 1610)	s3:authType (p. 1612)	
				s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
DeleteStorageLensConfigurationTags	Grants permission to remove tags from an existing Amazon S3 Storage Lens configuration	Tagging	storagelensconfiguration* (p. 1610)	s3:authType (p. 1612)	
				s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	

Service Authorization Reference
Service Authorization Reference
Amazon S3

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* (p. 1610)	s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
DescribeMultiRegionConfiguration	Grants permission to retrieve the configuration information for a multi-region access point	Read	multiregionaccesspointrequestarn* (p. 1610)	aws:RequestedRegion (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureversion (p. 1612) s3:signatureAge (p. 1612) s3:TlsVersion (p. 1612)	
GetAccelerateConfiguration	Grants permission to uses the <code>accelerate</code> subresource to return the Transfer Acceleration state of a bucket, which is either Enabled or Suspended	Read	bucket* (p. 1610)	s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	

Service Authorization Reference
 Service Authorization Reference
 Amazon S3

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 (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)
GetAccessPointConfigurationForObjectLambda	Grants permission to retrieve the configuration of the object lambda enabled access point	Read	objectlambdaaccesspoint* (p. 1610) s3:DataAccessPointArn (p. 1611) s3:DataAccessPointAccount (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)		
GetAccessPointForObjectLambda		Read	objectlambdaaccesspoint* (p. 1610)		

Service Authorization Reference
 Service Authorization Reference
 Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to create an object lambda enabled accesspoint			s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
GetAccessPointPolicy	Grants permission to returns the access point policy associated with the specified access point	Read	accesspoint* (p. 1610)	s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	

Service Authorization Reference
Service Authorization Reference
Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAccessPointPolicy	Grants permission to returns the access point policy associated with the specified object lambda enabled access point	Read	objectlambdaaccesspoint* (p. 1610)		
GetAccessPointPolicyStatus	Grants permission to return the policy status for a specific access point policy	Read	accesspoint* (p. 1610)		
GetAccessPointPolicyStatusForObjectLambda		Read	objectlambdaaccesspoint* (p. 1610)		

Service Authorization Reference
Service Authorization Reference
Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to return the policy status for a specific object lambda access point policy			s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
GetAccountPublicAccessBlock	Grants permission to retrieve the Public Access Block configuration for an AWS account	Read		s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
GetAnalyticsConfiguration	Grants permission to get an Analytics configuration from an Amazon S3 bucket, identified by the analytics configuration ID	Read	bucket* (p. 1610)		
			s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)		

Service Authorization Reference
 Service Authorization Reference
 Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetBucketAcl	Grants permission to use the acl subresource to return the access control list (ACL) of an Amazon S3 bucket	Read	bucket* (p. 1610) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)		
GetBucketCORS	Grants permission to return the CORS configuration information set for an Amazon S3 bucket	Read	bucket* (p. 1610) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)		
GetBucketLocation	Grants permission to return the Region that an Amazon S3 bucket resides in	Read	bucket* (p. 1610) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)		

Service Authorization Reference
Service Authorization Reference
Amazon S3

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* (p. 1610) 	s3:authType (p. 1612) 	
GetBucketNotification	Grants permission to get the notification configuration of an Amazon S3 bucket	Read	bucket* (p. 1610) 	s3:authType (p. 1612) 	
GetBucketObjectLockConfiguration	Grants permission to get the Object Lock configuration of an Amazon S3 bucket	Read	bucket* (p. 1610) 	s3:authType (p. 1612) 	
GetBucketOwnershipControls	Grants permission to retrieve ownership controls on a bucket	Read	bucket* (p. 1610)		

Service Authorization Reference
 Service Authorization Reference
 Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
GetBucketPolicy	Grants permission to return the policy of the specified bucket	Read	bucket* (p. 1610)	s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
GetBucketPolicyStatus	Grants permission to retrieve the policy status for a specific Amazon S3 bucket, which indicates whether the bucket is public	Read	bucket* (p. 1610)	s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
GetBucketPublicAccessBlock		Read	bucket* (p. 1610)		

Service Authorization Reference
Service Authorization Reference
Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to retrieve the PublicAccessBlock configuration for an Amazon S3 bucket			s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
GetBucketRequestPayment	Grants permission to return the request payment configuration for an Amazon S3 bucket	Read	bucket* (p. 1610)		
				s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
GetBucketTagging	Grants permission to return the tag set associated with an Amazon S3 bucket	Read	bucket* (p. 1610)		
				s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
GetBucketVersioning		Read	bucket* (p. 1610)		

Service Authorization Reference
Service Authorization Reference
Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to return the versioning state of an Amazon S3 bucket			s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
GetBucketWebsite	Grants permission to return the website configuration for an Amazon S3 bucket	Read	bucket* (p. 1610)		
				s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
GetEncryptionConfigurationDefault	Grants permission to return the encryption configuration for an Amazon S3 bucket	Read	bucket* (p. 1610)		
				s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	

Service Authorization Reference
Service Authorization Reference
Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetIntelligentTierList	Grants permission to get an or list all Amazon S3 Intelligent Tiering configuration in a S3 Bucket	Read	bucket* (p. 1610)		
GetInventoryConfiguration	Grants permission to return an inventory configuration from an Amazon S3 bucket, identified by the inventory configuration ID	Read	bucket* (p. 1610)		
GetJobTagging	Grants permission to return the tag set of an existing Amazon S3 Batch Operations job	Read	job* (p. 1610)		

Service Authorization Reference
Service Authorization Reference
Amazon S3

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* (p. 1610)		
		Read	bucket* (p. 1610)		
GetMultiRegionAccessPointConfiguration	Grants permission to return configuration information about the specified multi region access point	Read	multiregionaccesspoint* (p. 1610)		

Service Authorization Reference
Service Authorization Reference
Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetMultiRegionAccessPointPolicy	Grants permission to returns the access point policy associated with the specified multi region access point	Read	multiregionaccesspoint* (p. 1610)		
GetMultiRegionAccessPointPolicyStatusForStep	Grants permission to return the policy status for step specific multi region access point policy	Read	multiregionaccesspoint* (p. 1610)		
GetObject	Grants permission to retrieve objects from Amazon S3	Read	object* (p. 1610)		

Service Authorization Reference
 Service Authorization Reference
 Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:ExistingObjectTag/ <key> (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)
GetObjectAcl	Grants permission to return the access control list (ACL) of an object	Read	object* (p. 1610)		s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:ExistingObjectTag/ <key> (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)
	GetObjectAttributes	Read	object* (p. 1610)		

Service Authorization Reference
Service Authorization Reference
Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to retrieve attributes related to a specific object				s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:ExistingObjectTag/<key> (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)
GetObjectLegalHold	Grants permission to get an object's current Legal Hold status	Read	object* (p. 1610)		s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)
GetObjectRetention	Grants permission to retrieve the retention settings for an object	Read	object* (p. 1610)		

Service Authorization Reference
Service Authorization Reference
Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)
GetObjectTagging	Grants permission to return the tag set of an object	Read	object* (p. 1610)		s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:ExistingObjectTag/<key> (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)
GetObjectTorrent		Read	object* (p. 1610)		

Service Authorization Reference
 Service Authorization Reference
 Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to return torrent files from an Amazon S3 bucket			s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
GetObjectVersion	Grants permission to retrieve a specific version of an object	Read	object* (p. 1610)		
				s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:ExistingObjectTag/ <key> (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:versionid (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
GetObjectVersionAcl		Read	object* (p. 1610)		

Service Authorization Reference
 Service Authorization Reference
 Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to return the access control list (ACL) of a specific object version			s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:ExistingObjectTag/ <key> (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:versionid (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
GetObjectVersionAttributes	Grants permission to retrieve attributes related to a specific version of an object	Read	object* (p. 1610)	s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:ExistingObjectTag/ <key> (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:versionid (p. 1612) s3:x-amz-content-sha256 (p. 1612)	

Service Authorization Reference
Service Authorization Reference
Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetObjectVersionTorrent	Grants permission to replicate both plaintext objects and objects encrypted with SSE-S3 or SSE-KMS	Read	object* (p. 1610)	s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
GetObjectVersionTagSet	Grants permission to return the TagSet for a specific version of the object	Read	object* (p. 1610)	s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:ExistingObjectTag/<key> (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:versionid (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
GetObjectVersionTorrent		Read	object* (p. 1610)		

Service Authorization Reference
Service Authorization Reference
Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to get Torrent files about a different version using the <code>versionId</code> subresource			s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:versionid (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
GetReplicationConfiguration	Grants permission to get the <code>replication</code> configuration information set on an Amazon S3 bucket	Read	bucket* (p. 1610)	s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
GetStorageLensConfiguration	Grants permission to get an Amazon S3 Storage Lens configuration	Read	storageLensConfiguration* (p. 1610)	s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
GetStorageLensConfigurationTagging		Read	storageLensConfiguration* (p. 1610)		

Service Authorization Reference
Service Authorization Reference
Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to get the tag set of an existing Amazon S3 Storage Lens configuration			s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
GetStorageLensDashboard	Grants permission to get an Amazon S3 Storage Lens dashboard	Read	storagelensconfiguration* (p. 1610)	s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
InitiateReplication	Grants permission to initiate the replication process by setting replication status of an object to pending	Write	object* (p. 1610) s3:ResourceAccount (p. 1612)		
ListAccessPoints	Grants permission to list access points	List		s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	

Service Authorization Reference
Service Authorization Reference
Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAccessPointsForObject	Grants permission to list object accesspoints	List		s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
ListAllMyBuckets	Grants permission to list all buckets owned by the authenticated sender of the request	List		s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
ListBucket	Grants permission to list some or all of the objects in an Amazon S3 bucket (up to 1000)	List	bucket* (p. 1610)	s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:authType (p. 1612) s3:delimiter (p. 1612) s3:max-keys (p. 1612) s3:prefix (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	

Service Authorization Reference
Service Authorization Reference
Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListBucketMultipartUploads	Grants permission to list in-progress multipart uploads	List	bucket* (p. 1610)		
ListBucketVersions	Grants permission to list metadata about all the versions of objects in an Amazon S3 bucket	List	bucket* (p. 1610)		

Service Authorization Reference
Service Authorization Reference
Amazon S3

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 (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)
ListMultiRegionAccessPoints	Grants permission to list multi-region access points	List			aws:RequestedRegion (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureversion (p. 1612) s3:signatureAge (p. 1612) s3:TlsVersion (p. 1612)
ListMultipartUploadParts	Grants permission to list the parts that have been uploaded for a specific multipart upload	List	object* (p. 1610)		
					s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)

Service Authorization Reference
Service Authorization Reference
Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListStorageLensConfigurations	Grants permission to list Amazon S3 Storage Lens configurations	List		s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
ObjectOwnerOverrideReplicaOwnership	Grants permission to change replica ownership	Permissions management	object* (p. 1610)	s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
PutAccelerateConfiguration	Grants permission to use the <code>accelerate</code> subresource to set the Transfer Acceleration state of an existing S3 bucket	Write	bucket* (p. 1610)	s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
PutAccessPointConfigurationForObjectLambda		Write	objectlambdaaccesspoint* (p. 1610)		

Service Authorization Reference
 Service Authorization Reference
 Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to set the configuration of the object lambda enabled access point			s3:DataAccessPointArn (p. 1611) s3:DataAccessPointAccount (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
PutAccessPointPolicy	Grants permission to associate an access policy with a specified access point	Permissions management	accesspoint* (p. 1610)	s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	

Service Authorization Reference
Service Authorization Reference
Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutAccessPointPolicy	Grants permission to associate an access policy with a specified object lambda enabled access point	Permissions management	objectlambdaaccesspoint* (p. 1610)		s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)
PutAccessPointPublicAccessBlock	Grants permission to 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 (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)
PutAnalyticsConfiguration	Grants permission to set an analytics configuration for the bucket, specified by the analytics configuration ID	Write	bucket* (p. 1610)		
			s3:authType (p. 1612)	s3:ResourceAccount (p. 1612)	
			s3:signatureAge (p. 1612)	s3:signatureversion (p. 1612)	
			s3:TlsVersion (p. 1612)	s3:x-amz-content-sha256 (p. 1612)	

Service Authorization Reference
Service Authorization Reference
Amazon S3

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* (p. 1610)	s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-acl (p. 1612) s3:x-amz-content-sha256 (p. 1612) s3:x-amz-grant-full-control (p. 1612) s3:x-amz-grant-read (p. 1612) s3:x-amz-grant-read-acp (p. 1612) s3:x-amz-grant-write (p. 1613) s3:x-amz-grant-write-acp (p. 1613)	
PutBucketCORS	Grants permission to set the CORS configuration for an Amazon S3 bucket	Write	bucket* (p. 1610)	s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	

Service Authorization Reference
Service Authorization Reference
Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutBucketLogging	Grants permission to set the logging parameters for an Amazon S3 bucket	Write	bucket* (p. 1610) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)		
PutBucketNotification	Grants permission to receive notifications when certain events happen in an Amazon S3 bucket	Write	bucket* (p. 1610) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)		
PutBucketObjectLockConfiguration	Grants permission to put Object Lock configuration on a specific bucket	Write	bucket* (p. 1610) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:TlsVersion (p. 1612) s3:signatureversion (p. 1612)		
PutBucketOwnershipControls		Write	bucket* (p. 1610)		

Service Authorization Reference
Service Authorization Reference
Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to add, replace or delete ownership controls on a bucket			s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
PutBucketPolicy	Grants permission to add or replace a bucket policy on a bucket	Permissions management	bucket* (p. 1610)	s3:authType (p. 1612)	
PutBucketPublicAccessBlock	Grants permission to create or modify the PublicAccessBlock configuration for a specific Amazon S3 bucket	Permissions management	bucket* (p. 1610)	s3:authType (p. 1612)	
PutBucketRequestPayment		Write	bucket* (p. 1610)		

Service Authorization Reference
Service Authorization Reference
Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to set the request payment configuration of a bucket			s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
PutBucketTagging	Grants permission to add a set of tags to an existing Amazon S3 bucket	Tagging	bucket* (p. 1610)		
				s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	
PutBucketVersioning	Grants permission to set the versioning state of an existing Amazon S3 bucket	Write	bucket* (p. 1610)		
				s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	

Service Authorization Reference
Service Authorization Reference
Amazon S3

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* (p. 1610) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)		
PutEncryptionConfiguration	Grants permission to set the encryption configuration for an Amazon S3 bucket	Write	bucket* (p. 1610) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)		
PutIntelligentTieringUpdate	Grants permission to create new Intelligent Tiering or update or delete an existing Amazon S3 Intelligent Tiering configuration	Write	bucket* (p. 1610) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)		

Service Authorization Reference
Service Authorization Reference
Amazon S3

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* (p. 1610) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)		
PutJobTagging	Grants permission to replace tags on an existing Amazon S3 Batch Operations job	Tagging	job* (p. 1610) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612) s3:ExistingJobPriority (p. 1611) s3:ExistingJobOperation (p. 1611) aws:TagKeys (p. 1611) aws:RequestTag/\${TagKey} (p. 1611)		
PutLifecycleConfiguration	Grants permission to create a new lifecycle configuration for the bucket or replace an existing lifecycle configuration	Write	bucket* (p. 1610) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)		

Service Authorization Reference
Service Authorization Reference
Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutMetricsConfig update	Grants permission to set or update a metrics configuration for the CloudWatch request metrics from an Amazon S3 bucket	Write	bucket* (p. 1610)	s3:authType (p. 1612)	s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)
PutMultiRegionAccessPointPolicy	Grants permission to associate an access point policy with a specified multi region access point	Permissions management	multiregionaccesspoint* (p. 1610)	s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) aws:RequestedRegion (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureversion (p. 1612) s3:signatureAge (p. 1612) s3:TlsVersion (p. 1612)	
PutObject	Grants permission to add an object to a bucket	Write	object* (p. 1610)		

Service Authorization Reference
 Service Authorization Reference
 Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:RequestObjectTag/ <key> (p. 1611) s3:RequestObjectTagKeys (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-acl (p. 1612) s3:x-amz-content-sha256 (p. 1612) s3:x-amz-copy-source (p. 1612) s3:x-amz-grant-full-control (p. 1612) s3:x-amz-grant-read (p. 1612) s3:x-amz-grant-read-acp (p. 1612) s3:x-amz-grant-write (p. 1613) s3:x-amz-grant-write-acp (p. 1613)

Service Authorization Reference
 Service Authorization Reference
 Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:x-amz-metadata-directive (p. 1613) s3:x-amz-server-side-encryption (p. 1613) s3:x-amz-server-side-encryption-aws-kms-key-id (p. 1613) s3:x-amz-storage-class (p. 1613) s3:x-amz-website-redirect-location (p. 1613) s3:object-lock-mode (p. 1612) s3:object-lock-retain-until-date (p. 1612) s3:object-lock-remaining-retention-days (p. 1612) s3:object-lock-legal-hold (p. 1612)	

Service Authorization Reference
 Service Authorization Reference
 Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutObjectAcl	Grants permission to set the access control list (ACL) permissions for new or existing objects in an S3 bucket	Permissions management	object* (p. 1610)	s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:ExistingObjectTag/<key> (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-acl (p. 1612) s3:x-amz-content-sha256 (p. 1612) s3:x-amz-grant-full-control (p. 1612) s3:x-amz-grant-read (p. 1612) s3:x-amz-grant-read-acp (p. 1612) s3:x-amz-grant-write (p. 1613) s3:x-amz-grant-write-acp (p. 1613) s3:x-amz-storage-class (p. 1613)	
PutObjectLegalHold		Write	object* (p. 1610)		

Service Authorization Reference
 Service Authorization Reference
 Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to apply a Legal Hold configuration to the specified object			s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612) s3:object-lock-legal-hold (p. 1612)	
PutObjectRetention		Write	object* (p. 1610)		

Service Authorization Reference
 Service Authorization Reference
 Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to place an Object Retention configuration on an object			s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612) s3:object-lock-mode (p. 1612) s3:object-lock-retain-until-date (p. 1612) s3:object-lock-remaining-retention-days (p. 1612)	
PutObjectTagging		Tagging	object* (p. 1610)		

Service Authorization Reference
Service Authorization Reference
Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to set the supplied tag-set to an object that already exists in a bucket				s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:ExistingObjectTag/ <key> (p. 1611) s3:RequestObjectTag/ <key> (p. 1611) s3:RequestObjectTagKeys (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutObjectVersion	Grants permission to use the <code>acl</code> subresource to set the access control list (ACL) permissions for an object that already exists in a bucket	Permissions management	object* (p. 1610)	s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:ExistingObjectTag/<key> (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:versionid (p. 1612) s3:x-amz-acl (p. 1612) s3:x-amz-content-sha256 (p. 1612) s3:x-amz-grant-full-control (p. 1612) s3:x-amz-grant-read (p. 1612) s3:x-amz-grant-read-acp (p. 1612) s3:x-amz-grant-write (p. 1613) s3:x-amz-grant-write-acp (p. 1613) s3:x-amz-storage-class (p. 1613)	

Service Authorization Reference
Service Authorization Reference
Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutObjectVersionTagging	Grants permission to set the Supplied tag-set for a specific version of an object	Tagging	object* (p. 1610)		
PutReplicationConfiguration	Grants permission to create a new replication configuration or replace an existing one	Write	bucket* (p. 1610)	iam:PassRole	

Service Authorization Reference
Service Authorization Reference
Amazon S3

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 (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612) aws:TagKeys (p. 1611) aws:RequestTag/\${TagKey} (p. 1611)
PutStorageLensConfigurationTags	Grants permission to put or replace tags on an existing Amazon S3 Storage Lens configuration	Tagging	storagelensconfiguration* (p. 1610)		s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612) aws:TagKeys (p. 1611) aws:RequestTag/\${TagKey} (p. 1611)
ReplicateDelete	Grants permission to replicate delete markers to the destination bucket	Write	object* (p. 1610)		s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ReplicateObject	Grants permission to replicate objects and object tags to the destination bucket	Write	object* (p. 1610)	s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612) s3:x-amz-server-side-encryption (p. 1613) s3:x-amz-server-side-encryption-aws-kms-key-id (p. 1613)	
ReplicateTags	Grants permission to replicate object tags to the destination bucket	Tagging	object* (p. 1610)	s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)	

Service Authorization Reference
Service Authorization Reference
Amazon S3

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RestoreObject	Grants permission to restore an archived copy of an object back into Amazon S3	Write	object* (p. 1610)		s3:DataAccessPointAccount (p. 1611) s3:DataAccessPointArn (p. 1611) s3:AccessPointNetworkOrigin (p. 1611) s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612)
UpdateJobPriority	Grants permission to update the priority of an existing job	Write	job* (p. 1610)		s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612) s3:RequestJobPriority (p. 1611) s3:ExistingJobPriority (p. 1611) s3:ExistingJobOperation (p. 1611)
UpdateJobStatus	Grants permission to update the status for the specified job	Write	job* (p. 1610)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType (p. 1612) s3:ResourceAccount (p. 1612) s3:signatureAge (p. 1612) s3:signatureversion (p. 1612) s3:TlsVersion (p. 1612) s3:x-amz-content-sha256 (p. 1612) s3:ExistingJobPriority (p. 1611) s3:ExistingJobOperation (p. 1611) s3:JobSuspendedCause (p. 1611)	

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 \(p. 1552\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
accesspoint	arn:\${Partition}:s3:\${Region}: \${Account}:accesspoint/\${AccessPointName}	
bucket	arn:\${Partition}:s3::::\${BucketName}	
object	arn:\${Partition}:s3::::\${BucketName}/ \${ObjectName}	
job	arn:\${Partition}:s3:\${Region}: \${Account}:job/\${JobId}	
storagelensconfig	arn:\${Partition}:s3:\${Region}: \${Account}:storage-lens/\${ConfigId}	aws:ResourceTag/\${TagKey} (p. 1611)
objectlambdaaccesspoint	arn:\${Partition}:s3-object-lambda:\${Region}: \${Account}:accesspoint/\${AccessPointName}	
multiregionaccesspointalias	arn:\${Partition}:s3::::\${Account}:accesspoint/ \${AccessPointAlias}	
multiregionaccesspointasyncrequestmrap	arn:\${Partition}:s3:us-west-2: \${Account}:awsync-request/mrap/\${Operation}/ \${Token}	

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters access by the tags that are passed in the request	String
<code>aws:RequestedRegion</code>	Filters access by Requested region for the multi region access point operation	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters access by the tags associated with the resource	String
<code>aws:TagKeys</code>	Filters access by the tag keys that are passed in the request	ArrayOfString
<code>s3:AccessPointNetworkOrigin</code>	Filters access by the network origin (Internet or VPC)	String
<code>s3:DataAccessPointArn</code>	Filters access by the AWS Account ID that owns the access point	String
<code>s3:DataAccessPointArn</code>	Filters access by an access point Amazon Resource Name (ARN)	String
<code>s3:ExistingJobOperation</code>	Filters access by operation to updating the job priority	String
<code>s3:ExistingJobPriority</code>	Filters access by priority range to cancelling existing jobs	Numeric
<code>s3:ExistingObjectTag/<key></code>	Filters access by existing object tag key and value	String
<code>s3:JobSuspendedCause</code>	Filters access by a specific job suspended cause (for example, AWAITING_CONFIRMATION) to cancelling suspended jobs	String
<code>s3:LocationConstraint</code>	Filters access by a specific Region	String
<code>s3:RequestJobOperation</code>	Filters access by operation to creating jobs	String
<code>s3:RequestJobPriority</code>	Filters access by priority range to creating new jobs	Numeric
<code>s3:RequestObjectTagObjects/<key></code>	Filters access by the tag keys and values to be added to objects	String
<code>s3:RequestObjectTagKeys</code>	Filters access by the tag keys to be added to objects	ArrayOfString

Condition keys	Description	Type
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:VersionId	Filters access by a specific object version	String
s3:authType	Filters access by authentication method	String
s3:delimiter	Filters access by delimiter parameter	String
s3:locationconstraint	Filters access by a specific Region	String
s3:max-keys	Filters access by maximum number of keys returned in a ListBucket request	Numeric
s3:object-lock-legal-hold	Filters access by object legal hold status	String
s3:object-lock-mode	Filters access by object retention mode (COMPLIANCE or GOVERNANCE)	String
s3:object-lock-remaining-retention-days	Filters access by remaining object retention days	String
s3:object-lock-retain-until-date	Filters access by object retain-until date	String
s3:prefix	Filters access by key name prefix	String
s3:signatureAge	Filters access by the age in milliseconds of the request signature	Numeric
s3:signatureversion	Filters access by the version of AWS Signature used on the request	String
s3:versionid	Filters access by a specific object version	String
s3:x-amz-acl	Filters access by canned ACL in the request's x-amz-acl header	String
s3:x-amz-content-sha256	Filters access by unsigned content in your bucket	String
s3:x-amz-copy-source	Filters access by copy source bucket, prefix, or object in the copy object requests	String
s3:x-amz-grant-full-control	Filters access by x-amz-grant-full-control (full control) header	String
s3:x-amz-grant-read	Filters access by x-amz-grant-read (read access) header	String
s3:x-amz-grant-read-acp	Filters access by the x-amz-grant-read-acp (read permissions for the ACL) header	String

Condition keys	Description	Type
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	String
s3:x-amz-storage-class	Filters access by storage class	String
s3:x-amz-website-redirect-location	Filters access by a specific website redirect location for buckets that are configured as static websites	String

Actions, resources, and condition keys for Amazon S3 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 \(p. 1613\)](#)
- [Resource types defined by Amazon S3 Glacier \(p. 1616\)](#)
- [Condition keys for Amazon S3 Glacier \(p. 1616\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1616)		
AbortVaultLock	Grants permission to abort the vault locking process if the vault lock is not in the Locked state	Permissions management	vault* (p. 1616)		
AddTagsToVault	Grants permission to add the specified tags to a vault	Tagging	vault* (p. 1616)		
			aws:TagKeys (p. 1616)		
CompleteMultipartUpload	Grants permission to complete a multipart upload process	Write	vault* (p. 1616)		
			aws:RequestTag/ \${TagKey} (p. 1616)		
CompleteVaultLock	Grants permission to complete the vault locking process	Permissions management	vault* (p. 1616)		
			glacier:ArchiveAgeInDays (p. 1617)		
CreateVault	Grants permission to create a new vault with the specified name	Write	vault* (p. 1616)		
DeleteArchive	Grants permission to delete an archive from a vault	Write	vault* (p. 1616)		
			glacier:ArchiveAgeInDays (p. 1617)		
DeleteVault	Grants permission to delete a vault	Write	vault* (p. 1616)		
DeleteVaultAccessPolicy	Grants permission to delete the policy associated with the specified vault	Permissions management	vault* (p. 1616)		
DeleteVaultNotification	Grants permission to delete the notification configuration set for a vault	Write	vault* (p. 1616)		
DescribeJob	Grants permission to get information about a job previously initiated	Read	vault* (p. 1616)		
DescribeVault	Grants permission to get information about a vault	Read	vault* (p. 1616)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDataRetrievalPolicy	Grants permission to get the retrieval policy	Read			
GetJobOutput	Grants permission to download the output of the job specified	Read	vault* (p. 1616)		
GetVaultAccessPolicy	Grants permission to retrieve the access-policy subresource set on the vault	Read	vault* (p. 1616)		
GetVaultLock	Grants permission to retrieve attributes from the lock-policy subresource set on the specified vault	Read	vault* (p. 1616)		
GetVaultNotificationConfigurations	Grants permission to retrieve the notification-configuration subresource set on the vault	Read	vault* (p. 1616)		
InitiateJob	Grants permission to initiate a job of the specified type	Write	vault* (p. 1616)		
InitiateMultipartUpload	Grants permission to initiate a multipart upload		vault* (p. 1616)	glacier:ArchiveAgeInDays (p. 1617)	
InitiateVaultLock	Grants permission to initiate the vault locking process	Permissions management	vault* (p. 1616)		
ListJobs	Grants permission to list jobs for a vault that are in-progress and jobs that have recently finished	List	vault* (p. 1616)		
ListMultipartUploads	Grants permission to list in-progress multipart uploads for the specified vault	List	vault* (p. 1616)		
ListParts	Grants permission to list the parts of an archive that have been uploaded in a specific multipart upload	List	vault* (p. 1616)		
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* (p. 1616)		
ListVaults	Grants permission to list all vaults	List			
PurchaseProvisionedCapacity	Grants permission to purchase provisioned capacity unit for an AWS account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RemoveTagsFromVault	Grants permission to remove one or more tags from the set of tags attached to a vault	Tagging	vault* (p. 1616)		
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* (p. 1616)		
SetVaultNotifications	Grants permission to configure vault notifications	Write	vault* (p. 1616)		
UploadArchive	Grants permission to upload an archive to a vault	Write	vault* (p. 1616)		
UploadMultipartPart	Grants permission to upload a part of an archive	Write	vault* (p. 1616)		

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 \(p. 1613\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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 [Available global condition 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

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 \(p. 1617\)](#)
- [Resource types defined by Amazon S3 Object Lambda \(p. 1623\)](#)
- [Condition keys for Amazon S3 Object Lambda \(p. 1624\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1623) s3-object-lambda:authType (p. 1624)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-object-lambda:signatureAge (p. 1624)	
				s3-object-lambda:TlsVersion (p. 1624)	
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* (p. 1623)		
				s3-object-lambda:authType (p. 1624)	
				s3-object-lambda:signatureAge (p. 1624)	
				s3-object-lambda:TlsVersion (p. 1624)	
DeleteObjectTagging	Grants permission to use the <code>tagging</code> subresource to remove the entire tag set from the specified object	Tagging	objectlambdaaccesspoint* (p. 1623)		
				s3-object-lambda:authType (p. 1624)	
				s3-object-lambda:signatureAge (p. 1624)	
				s3-object-lambda:TlsVersion (p. 1624)	
DeleteObjectVersion	Grants permission to remove a specific version of an object	Write	objectlambdaaccesspoint* (p. 1623)		
				s3-object-lambda:authType (p. 1624)	
				s3-object-lambda:signatureAge (p. 1624)	
				s3-object-lambda:TlsVersion (p. 1624)	
				s3-object-lambda:versionid (p. 1624)	
DeleteObjectVersionTagging	Grants permission to remove the <code>Tagging</code> tag set for a specific version of the object	Tagging	objectlambdaaccesspoint* (p. 1623)		
				s3-object-lambda:authType (p. 1624)	
				s3-object-lambda:signatureAge (p. 1624)	
				s3-object-lambda:TlsVersion (p. 1624)	
				s3-object-lambda:versionid (p. 1624)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetObject	Grants permission to retrieve objects from Amazon S3	Read	objectlambdaaccesspoint* (p. 1623)	s3-object-lambda:authType (p. 1624)	s3-object-lambda:signatureAge (p. 1624)
GetObjectAcl	Grants permission to return the access control list (ACL) of an object	Read	objectlambdaaccesspoint* (p. 1623)	s3-object-lambda:authType (p. 1624)	s3-object-lambda:signatureAge (p. 1624)
GetObjectLegalHold	Grants permission to get an object's current Legal Hold status	Read	objectlambdaaccesspoint* (p. 1623)	s3-object-lambda:authType (p. 1624)	s3-object-lambda:signatureAge (p. 1624)
GetObjectRetention	Grants permission to retrieve the retention settings for an object	Read	objectlambdaaccesspoint* (p. 1623)	s3-object-lambda:authType (p. 1624)	s3-object-lambda:signatureAge (p. 1624)
GetObjectTagging	Grants permission to return the tag set of an object	Read	objectlambdaaccesspoint* (p. 1623)	s3-object-lambda:authType (p. 1624)	s3-object-lambda:signatureAge (p. 1624)
GetObjectVersion	Grants permission to retrieve a specific version of an object	Read	objectlambdaaccesspoint* (p. 1623)		

Service Authorization Reference
Service Authorization Reference
Amazon S3 Object Lambda

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-object-lambda:authType (p. 1624) s3-object-lambda:signatureAge (p. 1624) s3-object-lambda:TlsVersion (p. 1624) s3-object-lambda:versionid (p. 1624)	
GetObjectVersion Action	Grants permission to return the access control list (ACL) of a specific object version	Read	objectlambdaaccesspoint* (p. 1623)	s3-object-lambda:authType (p. 1624)	
			s3-object-lambda:signatureAge (p. 1624) s3-object-lambda:TlsVersion (p. 1624) s3-object-lambda:versionid (p. 1624)		
GetObjectVersion TagSet	Grants permission to return the TagSet for a specific version of the object	Read	objectlambdaaccesspoint* (p. 1623)	s3-object-lambda:authType (p. 1624)	
			s3-object-lambda:signatureAge (p. 1624) s3-object-lambda:TlsVersion (p. 1624) s3-object-lambda:versionid (p. 1624)		
ListBucket	Grants permission to list some or all of the objects in an Amazon S3 bucket (up to 1000)	List	objectlambdaaccesspoint* (p. 1623)	s3-object-lambda:authType (p. 1624)	
				s3-object-lambda:signatureAge (p. 1624) s3-object-lambda:TlsVersion (p. 1624)	
ListBucketMultipartUploads	Grants permission to list incomplete multipart uploads	List	objectlambdaaccesspoint* (p. 1623)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-object-lambda:authType (p. 1624) s3-object-lambda:signatureAge (p. 1624) s3-object-lambda:TlsVersion (p. 1624)	
ListBucketVersion	Grants permission to list metadata about all the versions of objects in an Amazon S3 bucket	List	objectlambdaaccesspoint* (p. 1623)		
				s3-object-lambda:authType (p. 1624) s3-object-lambda:signatureAge (p. 1624) s3-object-lambda:TlsVersion (p. 1624)	
ListMultipartUploadParts	Grants permission to list the parts that have been uploaded for a specific multipart upload	List	objectlambdaaccesspoint* (p. 1623)		
				s3-object-lambda:authType (p. 1624) s3-object-lambda:signatureAge (p. 1624) s3-object-lambda:TlsVersion (p. 1624)	
PutObject	Grants permission to add an object to a bucket	Write	objectlambdaaccesspoint* (p. 1623)		
				s3-object-lambda:authType (p. 1624) s3-object-lambda:signatureAge (p. 1624) s3-object-lambda:TlsVersion (p. 1624)	
PutObjectAcl	Grants permission to set the access control list (ACL) permissions for new or existing objects in an S3 bucket.	Permissions management	objectlambdaaccesspoint* (p. 1623)		
				s3-object-lambda:authType (p. 1624) s3-object-lambda:signatureAge (p. 1624) s3-object-lambda:TlsVersion (p. 1624)	
PutObjectLegalHold	Grants permission to apply a Legal Hold configuration to the specified object	Write	objectlambdaaccesspoint* (p. 1623)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-object-lambda:authType (p. 1624) s3-object-lambda:signatureAge (p. 1624) s3-object-lambda:TlsVersion (p. 1624)	
PutObjectRetention	Grants permission to place an Object Retention configuration on an object	Write	objectlambdaaccesspoint* (p. 1623)	s3-object-lambda:authType (p. 1624)	
				s3-object-lambda:signatureAge (p. 1624) s3-object-lambda:TlsVersion (p. 1624)	
PutObjectTagging	Grants permission to set the supplied tag-set to an object that already exists in a bucket	Tagging	objectlambdaaccesspoint* (p. 1623)	s3-object-lambda:authType (p. 1624)	
				s3-object-lambda:signatureAge (p. 1624) s3-object-lambda:TlsVersion (p. 1624)	
PutObjectVersion	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* (p. 1623)	s3-object-lambda:authType (p. 1624)	
				s3-object-lambda:signatureAge (p. 1624) s3-object-lambda:TlsVersion (p. 1624) s3-object-lambda:versionid (p. 1624)	
PutObjectVersionTagging	Grants permission to set the supplied tag-set for a specific version of an object	Tagging	objectlambdaaccesspoint* (p. 1623)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-object-lambda:authType (p. 1624) s3-object-lambda:signatureAge (p. 1624) s3-object-lambda:TlsVersion (p. 1624) s3-object-lambda:versionid (p. 1624)	
RestoreObject	Grants permission to restore an archived copy of an object back into Amazon S3	Write	objectlambdaaccesspoint* (p. 1623)	s3-object-lambda:authType (p. 1624)	
				s3-object-lambda:signatureAge (p. 1624)	s3-object-lambda:TlsVersion (p. 1624)
WriteGetObjectDataForGetObject	Grants permission to provide data for GetObject requests send to S3 Object Lambda	Write	objectlambdaaccesspoint* (p. 1623)	s3-object-lambda:authType (p. 1624)	
				s3-object-lambda:signatureAge (p. 1624)	s3-object-lambda:TlsVersion (p. 1624)

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 \(p. 1617\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
	arn:\${Partition}:s3-object-lambda:\${Region}:objectlambdaaccesspoint/\${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 [Available global condition keys](#).

Condition keys	Description	Type
<code>s3-object-lambda:TlsVersion</code>	Filters access by the TLS version used by the client	Numeric
<code>s3-object-lambda:authType</code>	Filters access by authentication method	String
<code>s3-object-lambda:signatureAgeSignature</code>	Filters access by the age in milliseconds of the request	Numeric
<code>s3-object-lambda:versionid</code>	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 \(p. 1624\)](#)
- [Resource types defined by Amazon S3 on Outposts \(p. 1640\)](#)
- [Condition keys for Amazon S3 on Outposts \(p. 1641\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1641)	s3-outposts:DataAccessPointArn (p. 1641) s3-outposts:DataAccessPointAccount (p. 1641) s3-outposts:AccessPointNetworkOrigin (p. 1641) s3-outposts:authType (p. 1641) s3-outposts:signatureAge (p. 1642) s3-outposts:signatureversion (p. 1642) s3-outposts:x-amz-content-sha256 (p. 1642)	
CreateAccessPoint	Grants permission to create a new access point	Write	accesspoint* (p. 1640)	s3-outposts:DataAccessPointAccount (p. 1641) s3-outposts:DataAccessPointArn (p. 1641) s3-outposts:AccessPointNetworkOrigin (p. 1641) s3-outposts:authType (p. 1641) s3-outposts:signatureAge (p. 1642) s3-outposts:signatureversion (p. 1642) s3-outposts:x-amz-	

Service Authorization Reference
Service Authorization Reference
Amazon S3 on Outposts

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				content-sha256 (p. 1642)	
CreateBucket	Grants permission to create a new bucket	Write	bucket* (p. 1641)		
			s3-outposts:authType (p. 1641)		
			s3-outposts:signatureAge (p. 1642)		
			s3-outposts:signatureversion (p. 1642)		
			s3-outposts:x-amz-content-sha256 (p. 1642)		
CreateEndpoint	Grants permission to create a new endpoint	Write	endpoint* (p. 1641)		
			accesspoint* (p. 1640)		
	Grants permission to delete the access point named in the URI	Write	s3-outposts:DataAccessPointArn (p. 1641)		
			s3-outposts:DataAccessPointAccount (p. 1641)		
			s3-outposts:AccessPointNetworkOrigin (p. 1641)		
			s3-outposts:authType (p. 1641)		
			s3-outposts:signatureAge (p. 1642)		
			s3-outposts:signatureversion (p. 1642)		
			s3-outposts:x-amz-content-sha256 (p. 1642)		
	Grants permission to delete the DeleteAccessPointPolicy on a specified access point	Permissions management	accesspoint* (p. 1640)		

Service Authorization Reference
 Service Authorization Reference
 Amazon S3 on Outposts

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-outposts:DataAccessPointArn (p. 1641) s3-outposts:DataAccessPointAccount (p. 1641) s3-outposts:AccessPointNetworkOrigin (p. 1641) s3-outposts:authType (p. 1641) s3-outposts:signatureAge (p. 1642) s3-outposts:signatureversion (p. 1642) s3-outposts:x-amz-content-sha256 (p. 1642)	
DeleteBucket	Grants permission to delete the bucket named in the URI	Write	bucket* (p. 1641)		
			s3-outposts:authType (p. 1641) s3-outposts:signatureAge (p. 1642) s3-outposts:signatureversion (p. 1642) s3-outposts:x-amz-content-sha256 (p. 1642)		
DeleteBucketPolicy	Grants permission to delete the policy on a specified bucket	Permissions management	bucket* (p. 1641)		

Service Authorization Reference
 Service Authorization Reference
 Amazon S3 on Outposts

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-outposts:authType (p. 1641) s3-outposts:signatureAge (p. 1642) s3-outposts:signatureversion (p. 1642) s3-outposts:x-amz-content-sha256 (p. 1642)	
DeleteEndpoint	Grants permission to delete the endpoint named in the URI	Write	endpoint* (p. 1641)		
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* (p. 1641) s3-outposts:DataAccessPointAccount (p. 1641) s3-outposts:DataAccessPointArn (p. 1641) s3-outposts:AccessPointNetworkOrigin (p. 1641) s3-outposts:authType (p. 1641) s3-outposts:signatureAge (p. 1642) s3-outposts:signatureversion (p. 1642) s3-outposts:x-amz-content-sha256 (p. 1642)		

Service Authorization Reference
 Service Authorization Reference
 Amazon S3 on Outposts

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteObjectTagging	Grants permission to use the <code>Tagging</code> subresource to remove the entire tag set from the specified object	Tagging	object* (p. 1641)	s3-outposts:DataAccessPointAccount (p. 1641)	
GetAccessPoint	Grants permission to return configuration information about the specified access point	Read		s3-outposts:DataAccessPointAccount (p. 1641)	
GetAccessPointPolicy		Read	accesspoint* (p. 1640)		

Service Authorization Reference
 Service Authorization Reference
 Amazon S3 on Outposts

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to returns the access point policy associated with the specified access point			s3-outposts:DataAccessPointAccount (p. 1641) s3-outposts:DataAccessPointArn (p. 1641) s3-outposts:AccessPointNetworkOrigin (p. 1641) s3-outposts:authType (p. 1641) s3-outposts:signatureAge (p. 1642) s3-outposts:signatureversion (p. 1642) s3-outposts:x-amz-content-sha256 (p. 1642)	
GetBucket	Grants permission to return the bucket configuration associated with an Amazon S3 bucket	Read	bucket* (p. 1641)		
				s3-outposts:authType (p. 1641) s3-outposts:signatureAge (p. 1642) s3-outposts:signatureversion (p. 1642) s3-outposts:x-amz-content-sha256 (p. 1642)	
GetBucketPolicy	Grants permission to return the policy of the specified bucket	Read	bucket* (p. 1641)		

Service Authorization Reference
Service Authorization Reference
Amazon S3 on Outposts

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-outposts:authType (p. 1641) s3-outposts:signatureAge (p. 1642) s3-outposts:signatureversion (p. 1642) s3-outposts:x-amz-content-sha256 (p. 1642)	
GetBucketTagging	Grants permission to return the tag set associated with an Amazon S3 bucket	Read	bucket* (p. 1641)	s3-outposts:authType (p. 1641) s3-outposts:signatureAge (p. 1642) s3-outposts:signatureversion (p. 1642) s3-outposts:x-amz-content-sha256 (p. 1642)	
GetLifecycleConfiguration	Grants permission to return the lifecycle configuration information set on an Amazon S3 bucket	Read	bucket* (p. 1641)	s3-outposts:authType (p. 1641) s3-outposts:signatureAge (p. 1642) s3-outposts:signatureversion (p. 1642) s3-outposts:x-amz-content-sha256 (p. 1642)	
GetObject	Grants permission to retrieve objects from Amazon S3	Read	object* (p. 1641)		

Service Authorization Reference
 Service Authorization Reference
 Amazon S3 on Outposts

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-outposts:DataAccessPointAccount (p. 1641) s3-outposts:DataAccessPointArn (p. 1641) s3-outposts:AccessPointNetworkOrigin (p. 1641) s3-outposts:ExistingObjectTag/<key> (p. 1641) s3-outposts:authType (p. 1641) s3-outposts:signatureAge (p. 1642) s3-outposts:signatureversion (p. 1642) s3-outposts:x-amz-content-sha256 (p. 1642)	
GetObjectTagging	Grants permission to return the tag set of an object	Read	object* (p. 1641)		

Service Authorization Reference
 Service Authorization Reference
 Amazon S3 on Outposts

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-outposts:DataAccessPointAccount (p. 1641) s3-outposts:DataAccessPointArn (p. 1641) s3-outposts:AccessPointNetworkOrigin (p. 1641) s3-outposts:ExistingObjectTag/<key> (p. 1641) s3-outposts:authType (p. 1641) s3-outposts:signatureAge (p. 1642) s3-outposts:signatureversion (p. 1642) s3-outposts:x-amz-content-sha256 (p. 1642)	
ListAccessPoints	Grants permission to list access points	List		s3-outposts:authType (p. 1641) s3-outposts:signatureAge (p. 1642) s3-outposts:signatureversion (p. 1642) s3-outposts:x-amz-content-sha256 (p. 1642)	
ListBucket	Grants permission to list some or all of the objects in an Amazon S3 bucket (up to 1000)	List	accesspoint* (p. 1640) bucket* (p. 1641)		

Service Authorization Reference
 Service Authorization Reference
 Amazon S3 on Outposts

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-outposts:DataAccessPointAccount (p. 1641) s3-outposts:DataAccessPointArn (p. 1641) s3-outposts:AccessPointNetworkOrigin (p. 1641) s3-outposts:authType (p. 1641) s3-outposts:delimiter (p. 1641) s3-outposts:max-keys (p. 1641) s3-outposts:prefix (p. 1641) s3-outposts:signatureAge (p. 1642) s3-outposts:signatureversion (p. 1642) s3-outposts:x-amz-content-sha256 (p. 1642)	
ListBucketMultipartUploads	Grants permission to list incomplete multipart uploads	List	accesspoint*	(p. 1640)	
			bucket*	(p. 1641)	

Service Authorization Reference
 Service Authorization Reference
 Amazon S3 on Outposts

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-outposts:DataAccessPointAccount (p. 1641) s3-outposts:DataAccessPointArn (p. 1641) s3-outposts:AccessPointNetworkOrigin (p. 1641) s3-outposts:authType (p. 1641) s3-outposts:signatureAge (p. 1642) s3-outposts:signatureversion (p. 1642) s3-outposts:x-amz-content-sha256 (p. 1642)	
ListEndpoints	Grants permission to list endpoints	List			
ListMultipartUploadParts	Grants permission to list the parts that have been uploaded for a specific multipart upload	List	object* (p. 1641) s3-outposts:DataAccessPointAccount (p. 1641) s3-outposts:DataAccessPointArn (p. 1641) s3-outposts:AccessPointNetworkOrigin (p. 1641) s3-outposts:authType (p. 1641) s3-outposts:signatureAge (p. 1642) s3-outposts:signatureversion (p. 1642) s3-outposts:x-amz-content-sha256 (p. 1642)		

Service Authorization Reference
Service Authorization Reference
Amazon S3 on Outposts

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListRegionalBuckets	Grants permission to list all buckets owned by the authenticated sender of the request	List		s3-outposts:authType (p. 1641) s3-outposts:signatureAge (p. 1642) s3-outposts:signatureversion (p. 1642) s3-outposts:x-amz-content-sha256 (p. 1642)	
ListSharedEndpoints	Grants permission to list shared endpoints	List			
PutAccessPointPolicy	Grants permission to associate an access policy with a specified access point	Permissions management	accesspoint* (p. 1640) s3-outposts:DataAccessPointAccount (p. 1641) s3-outposts:DataAccessPointArn (p. 1641) s3-outposts:AccessPointNetworkOrigin (p. 1641) s3-outposts:authType (p. 1641) s3-outposts:signatureAge (p. 1642) s3-outposts:signatureversion (p. 1642) s3-outposts:x-amz-content-sha256 (p. 1642)		
PutBucketPolicy	Grants permission to add or replace a bucket policy on a bucket	Permissions management	bucket* (p. 1641)		

Service Authorization Reference
Service Authorization Reference
Amazon S3 on Outposts

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-outposts:authType (p. 1641) s3-outposts:signatureAge (p. 1642) s3-outposts:signatureversion (p. 1642) s3-outposts:x-amz-content-sha256 (p. 1642)	
PutBucketTagging	Grants permission to add a set of tags to an existing Amazon S3 bucket	Tagging	bucket* (p. 1641)	s3-outposts:authType (p. 1641) s3-outposts:signatureAge (p. 1642) s3-outposts:signatureversion (p. 1642) s3-outposts:x-amz-content-sha256 (p. 1642)	
PutLifecycleConfiguration	Grants permission to create a new lifecycle configuration for the bucket or replace an existing lifecycle configuration	Write	bucket* (p. 1641)	s3-outposts:authType (p. 1641) s3-outposts:signatureAge (p. 1642) s3-outposts:signatureversion (p. 1642) s3-outposts:x-amz-content-sha256 (p. 1642)	
PutObject	Grants permission to add an object to a bucket	Write	object* (p. 1641)		

Service Authorization Reference
 Service Authorization Reference
 Amazon S3 on Outposts

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-outposts:DataAccessPointAccount (p. 1642) s3-outposts:DataAccessPointArn (p. 1641) s3-outposts:AccessPointNetworkOrigin (p. 1641) s3-outposts:RequestObjectTag/<key> (p. 1641) s3-outposts:RequestObjectTagKeys (p. 1641) s3-outposts:authType (p. 1641) s3-outposts:signatureAge (p. 1642) s3-outposts:signatureversion (p. 1642) s3-outposts:x-amz-acl (p. 1642) s3-outposts:x-amz-content-sha256 (p. 1642) s3-outposts:x-amz-copy-source (p. 1642) s3-outposts:x-amz-metadata-directive (p. 1642) s3-outposts:x-amz-server-side-encryption (p. 1642)	

Service Authorization Reference
Service Authorization Reference
Amazon S3 on Outposts

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-outposts:x-amz-storage-class (p. 1642)	
PutObjectAcl	Grants permission to set the access control list (ACL) permissions for an object that already exists in a bucket	Permissions management	object* (p. 1641)	s3-outposts:DataAccessPointAccount (p. 1642)	
PutObjectTagging	Grants permission to set the supplied tag-set to an object that already exists in a bucket	Tagging	object* (p. 1641)	s3-outposts:authType (p. 1641)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-outposts:DataAccessPointAccount (p. 1641) s3-outposts:DataAccessPointArn (p. 1641) s3-outposts:AccessPointNetworkOrigin (p. 1641) s3-outposts:ExistingObjectTag/<key> (p. 1641) s3-outposts:RequestObjectTag/<key> (p. 1641) s3-outposts:RequestObjectTagKeys (p. 1641) s3-outposts:authType (p. 1641) s3-outposts:signatureAge (p. 1642) s3-outposts:signatureversion (p. 1642) s3-outposts:x-amz-content-sha256 (p. 1642)	

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 \(p. 1624\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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}	

Resource types	ARN	Condition keys
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 [Available global condition keys](#).

Condition keys	Description	Type
s3-outposts:AccessPointNetworkOrigin	Filters access by the network origin (Internet or VPC)	String
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)	String
s3-outposts:ExistingObjectTag	Filters access by requiring that an existing object tag has a specific tag key and value <key>	String
s3-outposts:RequestObjectTags	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: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 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 \(p. 1642\)](#)
- [Resource types defined by Amazon SageMaker \(p. 1678\)](#)
- [Condition keys for Amazon SageMaker \(p. 1683\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddAssociation	Grants permission to associate a lineage entity (artifact, context, action, experiment, experiment-trial-component) to each other	Write	action* (p. 1682)		
			artifact* (p. 1682)		
			context* (p. 1682)		
			experiment* (p. 1682)		
			experiment-trial-component* (p. 1682)		
AddTags	Grants permission to add or overwrite one or more tags for the specified Amazon SageMaker resource	Tagging	action (p. 1682)		
			algorithm (p. 1680)		
			app (p. 1679)		
			app-image-config (p. 1679)		
			artifact (p. 1682)		
			automl-job (p. 1681)		
			code-repository (p. 1679)		
			context (p. 1682)		
			data-quality-job-definition (p. 1681)		
			device (p. 1678)		
			device-fleet (p. 1678)		
			domain (p. 1679)		

Service Authorization Reference
 Service Authorization Reference
 Amazon SageMaker

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			edge-packaging-job (p. 1678)		
			endpoint (p. 1681)		
			endpoint-config (p. 1681)		
			experiment (p. 1682)		
			experiment-trial (p. 1682)		
			experiment-trial-component (p. 1682)		
			feature-group (p. 1682)		
			flow-definition (p. 1678)		
			human-task-ui (p. 1678)		
			hyper-parameter-tuning-job (p. 1680)		
			image (p. 1680)		
			inference-recommendations-job (p. 1678)		
			labeling-job (p. 1678)		
			model (p. 1680)		
			model-bias-job-definition (p. 1681)		
			model-explainability-job-definition (p. 1681)		
			model-package (p. 1680)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			model-package-group (p. 1680)		
			model-quality-job-definition (p. 1681)		
			monitoring-schedule (p. 1681)		
			notebook-instance (p. 1679)		
			pipeline (p. 1682)		
			processing-job (p. 1680)		
			project (p. 1680)		
			training-job (p. 1680)		
			transform-job (p. 1681)		
			user-profile (p. 1679)		
			workteam (p. 1678)		
				aws:RequestTag/\${TagKey} (p. 1683)	
					aws:TagKeys (p. 1683)
AssociateTrialComponent	Grants permission to associate a component with a trial	Write	experiment-trial* (p. 1682)		
				experiment-trial-component* (p. 1682)	
BatchDescribeModelPackages	Grants permission to describe ModelPackages	Read	model-package* (p. 1680)		
BatchGetMetrics [permission only]	Grants permission to retrieve metrics associated with SageMaker Resources such as Training Jobs. This API is not publicly exposed at this point, however admins can control this action	Read	training-job* (p. 1680)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetRecord	Grants permission to get a batch of records from one or more feature groups	Read	feature-group* (p. 1682)		
BatchPutMetrics [permission only]	Grants permission to publish metrics associated with a SageMaker Resource such as a Training Job. This API is not publicly exposed at this point, however admins can control this action	Write	training-job* (p. 1680)		
CreateAction	Grants permission to create an action	Write	action* (p. 1682)		
				aws:RequestTag/\${TagKey} (p. 1683)	aws:TagKeys (p. 1683)
CreateAlgorithm	Grants permission to create an algorithm	Write	algorithm* (p. 1680)		
				aws:RequestTag/\${TagKey} (p. 1683)	aws:TagKeys (p. 1683)
CreateApp	Grants permission to create an App for a SageMaker Studio UserProfile	Write	app* (p. 1679)		
				aws:RequestTag/\${TagKey} (p. 1683)	
				aws:TagKeys (p. 1683)	
				sagemaker:InstanceTypes (p. 1684)	
				sagemaker:ImageArns (p. 1683)	
				sagemaker:ImageVersionArns (p. 1684)	
CreateAppImageConfig	Grants permission to create an AppImageConfig	Write	app-image-config* (p. 1679)		
				aws:RequestTag/\${TagKey} (p. 1683)	aws:TagKeys (p. 1683)
CreateArtifact	Grants permission to create an artifact	Write	artifact* (p. 1682)		
				aws:RequestTag/\${TagKey} (p. 1683)	
				aws:TagKeys (p. 1683)	

Service Authorization Reference
Service Authorization Reference
Amazon SageMaker

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAutoMLJob	Grants permission to create an AutoML job	Write	automl-job* (p. 1681)		iam:PassRole
				aws:RequestTag/\${TagKey} (p. 1683)	
				aws:TagKeys (p. 1683)	
	Grants permission to create a CodeRepository	Write	code-repository* (p. 1679)		
				aws:RequestTag/\${TagKey} (p. 1683)	
				aws:TagKeys (p. 1683)	
CreateCompilationJob	Grants permission to create a compilation job	Write	compilation-job* (p. 1681)		iam:PassRole
				aws:RequestTag/\${TagKey} (p. 1683)	
				aws:TagKeys (p. 1683)	
CreateContext	Grants permission to create a context	Write	context* (p. 1682)		
				aws:RequestTag/\${TagKey} (p. 1683)	
				aws:TagKeys (p. 1683)	
CreateDataQualityJobDefinition	Grants permission to create a data quality job definition	Write	data-quality-job-definition* (p. 1681)		iam:PassRole

Service Authorization Reference
Service Authorization Reference
Amazon SageMaker

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					aws:RequestTag/\${TagKey} (p. 1683) aws:TagKeys (p. 1683) sagemaker:InstanceTypes (p. 1684) sagemaker:InterContainerTrafficEncryption (p. 1684) sagemaker:MaxRuntimeInSeconds (p. 1684) sagemaker:NetworkIsolation (p. 1684) sagemaker:OutputKmsKey (p. 1684) sagemaker:VolumeKmsKey (p. 1684) sagemaker:VpcSecurityGroupIds (p. 1684) sagemaker:VpcSubnets (p. 1684)
CreateDeviceFleet	Grants permission to create a device fleet	Write	device-fleet* (p. 1678)		iam:PassRole
					aws:RequestTag/\${TagKey} (p. 1683) aws:TagKeys (p. 1683)
CreateDomain	Grants permission to create a Domain for SageMaker Studio	Write	domain* (p. 1679)		iam:CreateServiceLinkedRole (p. 1684) iam:PassRole
					aws:RequestTag/\${TagKey} (p. 1683) aws:TagKeys (p. 1683) sagemaker:AppNetworkAccessType (p. 1684) sagemaker:InstanceTypes (p. 1684) sagemaker:VpcSecurityGroupIds (p. 1684) sagemaker:VpcSubnets (p. 1684) sagemaker:DomainSharingOutputKmsKey (p. 1684) sagemaker:VolumeKmsKey (p. 1684) sagemaker:ImageArns (p. 1683) sagemaker:ImageVersionArns (p. 1684)
CreateEdgePackagingJob	Grants permission to create an edge packaging job	Write	edge-packaging-job* (p. 1678)		iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 1683) aws:TagKeys (p. 1683)	
CreateEndpoint	Grants permission to create an endpoint using the endpoint configuration specified in the request	Write	endpoint* (p. 1681)		
	aws:RequestTag/ \${TagKey} (p. 1683) aws:TagKeys (p. 1683)				
CreateEndpointConfig	Grants permission to create an endpoint configuration that can be deployed using Amazon SageMaker hosting services	Write	endpoint- config* (p. 1681)		
	aws:RequestTag/ \${TagKey} (p. 1683) aws:TagKeys (p. 1683) sagemaker:AcceleratorTypes (p. 1683) sagemaker:InstanceTypes (p. 1684) sagemaker:ModelArn (p. 1684) sagemaker:VolumeKmsKey (p. 1684) sagemaker:ServerlessMaxConcurrency sagemaker:ServerlessMemorySize (p. 1684)				
CreateExperiment	Grants permission to create an experiment	Write	experiment* (p. 1682)		
	aws:RequestTag/ \${TagKey} (p. 1683) aws:TagKeys (p. 1683)				
CreateFeatureGroup	Grants permission to create a feature group	Write	feature- group* (p. 1682)		iam:PassRole
	aws:RequestTag/ \${TagKey} (p. 1683) aws:TagKeys (p. 1683) sagemaker:FeatureGroupOnlineStoreK sagemaker:FeatureGroupOfflineStoreK sagemaker:FeatureGroupOfflineStoreS				
CreateFlowDefinition	Grants permission to create a flow definition, which defines settings for a human workflow	Write	flow- definition* (p. 1678)		iam:PassRole

Service Authorization Reference
Service Authorization Reference
Amazon SageMaker

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					sagemaker:WorkteamArn (p. 1684) sagemaker:WorkteamType (p. 1684) aws:RequestTag/\${TagKey} (p. 1683) aws:TagKeys (p. 1683)
CreateHumanTaskUI	Grants permission to define the settings you will use for the human review workflow user interface	Write	human-task-ui* (p. 1678)		
					aws:RequestTag/\${TagKey} (p. 1683) aws:TagKeys (p. 1683)
CreateHyperParameterTuningJob	Grants permission to create a hyperparameter tuning job that can be deployed using Amazon SageMaker	Write	hyper-parameter-tuning-job* (p. 1680)		iam:PassRole
					aws:RequestTag/\${TagKey} (p. 1683) aws:TagKeys (p. 1683) sagemaker:FileSystemAccessMode (p. 1683) sagemaker:FileSystemDirectoryPath (p. 1683) sagemaker:FileSystemId (p. 1683) sagemaker:FileSystemType (p. 1683) sagemaker:InstanceTypes (p. 1684) sagemaker:InterContainerTrafficEncryption (p. 1684) sagemaker:MaxRuntimeInSeconds (p. 1684) sagemaker:NetworkIsolation (p. 1684) sagemaker:OutputKmsKey (p. 1684) sagemaker:VolumeKmsKey (p. 1684) sagemaker:VpcSecurityGroupIds (p. 1684) sagemaker:VpcSubnets (p. 1684)
CreateImage	Grants permission to create a SageMaker Image	Write	image* (p. 1680)		iam:PassRole

Service Authorization Reference
Service Authorization Reference
Amazon SageMaker

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/\${TagKey} (p. 1683) aws:TagKeys (p. 1683)	
CreateImageVersion	Grants permission to create a SageMaker ImageVersion	Write	image* (p. 1680)		
CreateInferenceRecommendationsJob	Grants permission to create an inference recommendations job	Write	inference-recommendations-job* (p. 1678)		iam:PassRole
				aws:RequestTag/\${TagKey} (p. 1683) aws:TagKeys (p. 1683)	
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* (p. 1678)		iam:PassRole
				sagemaker:WorkteamArn (p. 1684) sagemaker:WorkteamType (p. 1684) sagemaker:VolumeKmsKey (p. 1684) sagemaker:OutputKmsKey (p. 1684) aws:RequestTag/\${TagKey} (p. 1683) aws:TagKeys (p. 1683)	
CreateLineageGroupPolicy	Grants permission to create a lineage group policy	Write			
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* (p. 1680)		iam:PassRole
				aws:RequestTag/\${TagKey} (p. 1683) aws:TagKeys (p. 1683) sagemaker:NetworkIsolation (p. 1684) sagemaker:VpcSecurityGroupIds (p. 1684) sagemaker:VpcSubnets (p. 1684)	
CreateModelBiasJobDefinition	Grants permission to create a model bias job definition	Write	model-bias-job-definition* (p. 1681)		iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					aws:RequestTag/\${TagKey} (p. 1683) aws:TagKeys (p. 1683) sagemaker:InstanceTypes (p. 1684) sagemaker:InterContainerTrafficEncryption (p. 1684) sagemaker:MaxRuntimeInSeconds (p. 1684) sagemaker:NetworkIsolation (p. 1684) sagemaker:OutputKmsKey (p. 1684) sagemaker:VolumeKmsKey (p. 1684) sagemaker:VpcSecurityGroupIds (p. 1684) sagemaker:VpcSubnets (p. 1684)
CreateModelExplainabilityJobDefinition	Grants permission to create a model-explainability job definition	Write	model-explainability-job-definition* (p. 1681)		iam:PassRole
CreateModelPackage	Grants permission to create a ModelPackage	Write	model-package (p. 1680) model-package-group (p. 1680)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/\${TagKey} (p. 1683) aws:TagKeys (p. 1683) sagemaker:ModelApprovalStatus (p. 1683)	
CreateModelPackageGroup	Grants permission to create a Model Package Group	Write	model-package-group* (p. 1680)		
	aws:RequestTag/\${TagKey} (p. 1683) aws:TagKeys (p. 1683)				
CreateModelQualityJobDefinition	Grants permission to create a Model Quality job definition	Write	model-quality-job-definition* (p. 1681)		iam:PassRole
	aws:RequestTag/\${TagKey} (p. 1683) aws:TagKeys (p. 1683) sagemaker:InstanceTypes (p. 1684) sagemaker:InterContainerTrafficEncryption (p. 1684) sagemaker:MaxRuntimeInSeconds (p. 1684) sagemaker:NetworkIsolation (p. 1684) sagemaker:OutputKmsKey (p. 1684) sagemaker:VolumeKmsKey (p. 1684) sagemaker:VpcSecurityGroupIds (p. 1684) sagemaker:VpcSubnets (p. 1684)				
CreateMonitoringSchedule	Grants permission to create a Monitoring schedule	Write	monitoring-schedule* (p. 1681)		iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					aws:RequestTag/\${TagKey} (p. 1683) aws:TagKeys (p. 1683) sagemaker:InstanceTypes (p. 1684) sagemaker:InterContainerTrafficEncryption (p. 1684) sagemaker:MaxRuntimeInSeconds (p. 1684) sagemaker:NetworkIsolation (p. 1684) sagemaker:OutputKmsKey (p. 1684) sagemaker:VolumeKmsKey (p. 1684) sagemaker:VpcSecurityGroupIds (p. 1684) sagemaker:VpcSubnets (p. 1684)
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* (p. 1679)		iam:PassRole
	aws:RequestTag/\${TagKey} (p. 1683) aws:TagKeys (p. 1683) sagemaker:AcceleratorTypes (p. 1683) sagemaker:DirectInternetAccess (p. 1684) sagemaker:InstanceTypes (p. 1684) sagemaker:RootAccess (p. 1684) sagemaker:VolumeKmsKey (p. 1684) sagemaker:VpcSecurityGroupIds (p. 1684) sagemaker:VpcSubnets (p. 1684)				
CreateNotebookInstanceLifecycleConfig	Grants permission to create a notebook instance lifecycle configuration that can be deployed using Amazon SageMaker	Write	notebook-instance-lifecycle-config* (p. 1679)		
CreatePipeline	Grants permission to create a pipeline	Write	pipeline* (p. 1682)		iam:PassRole
	aws:RequestTag/\${TagKey} (p. 1683) aws:TagKeys (p. 1683)				

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePresignedDomainUrl	Grants permission to return a URL that you can use from your browser to connect to the Domain as a specified UserProfile when AuthMode is 'IAM'	Write	user-profile* (p. 1679)		
CreatePresignedNotebookInstanceUrl	Grants permission to create a URL that you can use from your browser to connect to the Notebook Instance	Write	notebook-instance* (p. 1679)		
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* (p. 1680)		iam:PassRole
			aws:RequestTag/\${TagKey} (p. 1683) aws:TagKeys (p. 1683) sagemaker:InstanceTypes (p. 1684) sagemaker:MaxRuntimeInSeconds (p. 1684) sagemaker:NetworkIsolation (p. 1684) sagemaker:OutputKmsKey (p. 1684) sagemaker:VolumeKmsKey (p. 1684) sagemaker:VpcSecurityGroupIds (p. 1684) sagemaker:VpcSubnets (p. 1684) sagemaker:InterContainerTrafficEncryption (p. 1684)		
CreateProject	Grants permission to create a Project	Write	project* (p. 1680)		
			aws:RequestTag/\${TagKey} (p. 1683) aws:TagKeys (p. 1683)		
CreateStudioLifecycleConfig	Grants permission to create a Studio Lifecycle Configuration that can be deployed using Amazon SageMaker	Write	studio-lifecycle-config* (p. 1679)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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* (p. 1680)		iam:PassRole
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* (p. 1681)		
CreateTrial	Grants permission to create a trial	Write	experiment-trial* (p. 1682)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTrialComponent	Grants permission to create a trial component	Write	experiment-trial-component* (p. 1682)		
			aws:RequestTag/\${TagKey} (p. 1683)	aws:TagKeys (p. 1683)	
CreateUserProfile	Grants permission to create a UserProfile for a SageMaker Studio Domain	Write	user-profile* (p. 1679)		iam:PassRole
			aws:RequestTag/\${TagKey} (p. 1683) aws:TagKeys (p. 1683)	sagemaker:VpcSecurityGroupIds (p. 1683) sagemaker:InstanceTypes (p. 1684) sagemaker:DomainSharingOutputKms (p. 1684) sagemaker:ImageArns (p. 1683) sagemaker:ImageVersionArns (p. 1684)	
CreateWorkforce	Grants permission to create a workforce	Write	workforce* (p. 1679)		
			aws:RequestTag/\${TagKey} (p. 1683)	aws:TagKeys (p. 1683)	
CreateWorkteam	Grants permission to create a workteam	Write	workteam* (p. 1678)		
			aws:RequestTag/\${TagKey} (p. 1683)	aws:TagKeys (p. 1683)	
DeleteAction	Grants permission to delete an action	Write	action* (p. 1682)		
DeleteAlgorithm	Grants permission to delete an algorithm	Write	algorithm* (p. 1680)		
DeleteApp	Grants permission to delete an App	Write	app* (p. 1679)		
DeleteAppImageConfig	Grants permission to delete an AppImageConfig	Write	app-image-config* (p. 1679)		
DeleteArtifact	Grants permission to delete an artifact	Write	artifact* (p. 1682)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAssociation	Grants permission to delete the association from a lineage entity (artifact, context, action, experiment, experiment-trial-component) to another	Write	action* (p. 1682) artifact* (p. 1682) context* (p. 1682) experiment* (p. 1682) experiment-trial-component* (p. 1682)		
DeleteCodeRepository	Grants permission to delete a CodeRepository	Write	code-repository* (p. 1679)		
DeleteContext	Grants permission to delete a context	Write	context* (p. 1682)		
DeleteDataQualityJobDefinition	Grants permission to delete a data quality job definition created using the CreateDataQualityJobDefinition API	Write	data-quality-job-definition* (p. 1681)		
DeleteDeviceFleet	Grants permission to delete a device fleet	Write	device-fleet* (p. 1678)		
DeleteDomain	Grants permission to delete a Domain	Write	domain* (p. 1679)		
DeleteEndpoint	Grants permission to delete an endpoint. Amazon SageMaker frees up all the resources that were deployed when the endpoint was created	Write	endpoint* (p. 1681)		
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* (p. 1681)		
DeleteExperiment	Grants permission to delete an experiment	Write	experiment* (p. 1682)		
DeleteFeatureGroup	Grants permission to delete a feature group	Write	feature-group* (p. 1682)		
aws:RequestTag/\${TagKey} (p. 1683)					
DeleteFlowDefinition	Grants permission to delete the specified flow definition	Write	flow-definition* (p. 1678)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteHumanLoop	Grants permission to delete a specified human loop	Write	human-loop* (p. 1678)		
DeleteHumanTaskUI	Grants permission to delete the specified human task user interface (worker task template)	Write	human-task-ui* (p. 1678)		
DeleteImage	Grants permission to delete a SageMaker Image	Write	image* (p. 1680)		
DeleteImageVersion	Grants permission to delete a SageMaker ImageVersion	Write	image-version* (p. 1680)		
DeleteLineageGroupPolicy	Grants permission to delete a lineage group policy	Write			
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* (p. 1680)		
DeleteModelBiasJobDefinition	Grants permission to delete a model bias job definition created using the CreateModelBiasJobDefinition API	Write	model-bias-job-definition* (p. 1681)		
DeleteModelExplainabilityJobDefinition	Grants permission to delete the model explainability job definition created using the CreateModelExplainabilityJobDefinition API	Write	model-explainability-job-definition* (p. 1681)		
DeleteModelPackage	Grants permission to delete a ModelPackage	Write	model-package* (p. 1680)		
DeleteModelPackageGroup	Grants permission to delete a ModelPackageGroup	Write	model-package-group* (p. 1680)		
DeleteModelPackageGroupPolicy	Grants permission to delete a ModelPackageGroup policy	Write	model-package-group* (p. 1680)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteModelQualityJobDefinition	Grants permission to delete the model quality job definition created using the CreateModelQualityJobDefinition API	Write	model-quality-job-definition* (p. 1681)		
DeleteMonitoringSchedule	Grants permission to delete a monitoring schedule	Write	monitoring-schedule* (p. 1681)		
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* (p. 1679)		
DeleteNotebookInstanceLifecycleConfig	Grants permission to delete a notebook instance lifecycle configuration	Write	notebook-instance-lifecycle-config* (p. 1679)		
DeletePipeline	Grants permission to delete a pipeline	Write	pipeline* (p. 1682)		
DeleteProject	Grants permission to delete a project	Write	project* (p. 1680)		
DeleteRecord	Grants permission to delete a record from a feature group	Write	feature-group* (p. 1682)		
DeleteStudioLifecycleConfiguration	Grants permission to delete a Studio Lifecycle Configuration	Write	studio-lifecycle-config* (p. 1679)		
DeleteTags	Grants permission to delete the specified set of tags from an Amazon SageMaker resource	Tagging	action (p. 1682)		
algorithm (p. 1680)					
app (p. 1679)					
app-image-config (p. 1679)					
artifact (p. 1682)					
automl-job (p. 1681)					
code-repository (p. 1679)					
compilation-job (p. 1681)					
context (p. 1682)					

Service Authorization Reference
 Service Authorization Reference
 Amazon SageMaker

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			data-quality-job-definition (p. 1681)		
			device (p. 1678)		
			device-fleet (p. 1678)		
			domain (p. 1679)		
			edge-packaging-job (p. 1678)		
			endpoint (p. 1681)		
			endpoint-config (p. 1681)		
			experiment (p. 1682)		
			experiment-trial (p. 1682)		
			experiment-trial-component (p. 1682)		
			feature-group (p. 1682)		
			flow-definition (p. 1678)		
			human-task-ui (p. 1678)		
			hyper-parameter-tuning-job (p. 1680)		
			image (p. 1680)		
			inference-recommendations-job (p. 1678)		
			labeling-job (p. 1678)		
			model (p. 1680)		

Service Authorization Reference
Service Authorization Reference
Amazon SageMaker

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			model-bias-job-definition (p. 1681)		
			model-explainability-job-definition (p. 1681)		
			model-package (p. 1680)		
			model-package-group (p. 1680)		
			model-quality-job-definition (p. 1681)		
			monitoring-schedule (p. 1681)		
			notebook-instance (p. 1679)		
			pipeline (p. 1682)		
			processing-job (p. 1680)		
			project (p. 1680)		
			training-job (p. 1680)		
			transform-job (p. 1681)		
			user-profile (p. 1679)		
			workteam (p. 1678)		
			aws:TagKeys (p. 1683)		
DeleteTrial	Grants permission to delete a trial	Write	experiment-trial* (p. 1682)		
DeleteTrialComponent	Grants permission to delete a trial component	Write	experiment-trial-component* (p. 1682)		
DeleteUserProfile	Grants permission to delete a user profile	Write	user-profile* (p. 1679)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteWorkforce	Grants permission to delete a workforce	Write	workforce* (p. 1679)		
DeleteWorkteam	Grants permission to delete a workteam	Write	workteam* (p. 1678)		
DeregisterDevices	Grants permission to deregister a set of devices	Write	device* (p. 1678)		
DescribeAction	Grants permission to get information about an action	Read	action* (p. 1682)		
DescribeAlgorithm	Grants permission to describe an algorithm	Read	algorithm* (p. 1680)		
DescribeApp	Grants permission to describe an App	Read	app* (p. 1679)		
DescribeAppImageConfig	Grants permission to describe an AppImageConfig	Read	app-image-config* (p. 1679)		
DescribeArtifact	Grants permission to get information about an artifact	Read	artifact* (p. 1682)		
DescribeAutoMLJob	Grants permission to describe an AutoML job that was created via the CreateAutoMLJob API	Read	automl-job* (p. 1681)		
DescribeCodeRepository	Grants permission to describe a CodeRepository	Read	code-repository* (p. 1679)		
DescribeCompilationJob	Grants permission to return information about a compilation job	Read	compilation-job* (p. 1681)		
DescribeContext	Grants permission to get information about a context	Read	context* (p. 1682)		
DescribeDataQualityJobDefinition	Grants permission to return information about a data quality job definition	Read	data-quality-job-definition* (p. 1681)		
DescribeDevice	Grants permission to access information about a device	Read	device* (p. 1678)		
DescribeDeviceFleet	Grants permission to access information about a device fleet	Read	device-fleet* (p. 1678)		
DescribeDomain	Grants permission to describe a Domain	Read	domain* (p. 1679)		
DescribeEdgePackagingJob	Grants permission to access information about an edge packaging job	Read	edge-packaging-job* (p. 1678)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeEndpoint	Grants permission to return the description of an endpoint	Read	endpoint* (p. 1681)		
DescribeEndpointConfig	Grants permission to return the description of an endpoint configuration, which was created using the CreateEndpointConfig API	Read	endpoint-config* (p. 1681)		
DescribeExperiment	Grants permission to return information about an experiment	Read	experiment* (p. 1682)		
DescribeFeatureGroup	Grants permission to return information about a feature group	Read	feature-group* (p. 1682)		
DescribeFlowDefinition	Grants permission to return information about the specified flow definition	Read	flow-definition* (p. 1678)		
DescribeHumanLoop	Grants permission to return information about the specified human loop	Read	human-loop* (p. 1678)		
DescribeHumanTaskUI	Grants permission to return detailed information about the specified human review workflow user interface	Read	human-task-ui* (p. 1678)		
DescribeHyperParameterTuningJob	Grants permission to describe a hyperparameter tuning job that was created via the CreateHyperParameterTuningJob API	Read	hyper-parameter-tuning-job* (p. 1680)		
DescribeImage	Grants permission to return information about a SageMaker Image	Read	image* (p. 1680)		
DescribeImageVersion	Grants permission to return information about a SageMaker ImageVersion	Read	image-version* (p. 1680)		
DescribeInferenceRecommendationsJob	Grants permission to get information about an inference recommendations job	Read	inference-recommendations-job* (p. 1678)		
DescribeLabelingJob	Grants permission to return information about a labeling job	Read	labeling-job* (p. 1678)		
DescribeLineageGroup	Grants permission to describe a lineage group	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeModel	Grants permission to describe a model that you created using the CreateModel API	Read	model* (p. 1680)		
DescribeModelBiasJobDefinition	Grants permission to return information about a model bias job definition	Read	model-bias-job-definition* (p. 1681)		
DescribeModelExplainabilityJobDefinition	Grants permission to return information about a model explainability job definition	Read	model-explainability-job-definition* (p. 1681)		
DescribeModelPackage	Grants permission to describe a ModelPackage	Read	model-package* (p. 1680)		
DescribeModelPackageGroup	Grants permission to describe a ModelPackageGroup	Read	model-package-group* (p. 1680)		
DescribeModelQualityJobDefinition	Grants permission to return information about a model quality job definition	Read	model-quality-job-definition* (p. 1681)		
DescribeMonitoringSchedule	Grants permission to return information about a monitoring schedule	Read	monitoring-schedule* (p. 1681)		
DescribeNotebookInstance	Grants permission to return information about a notebook instance	Read	notebook-instance* (p. 1679)		
DescribeNotebookInstanceLifecycleConfig	Grants permission to describe a notebook instance lifecycle configuration that was created via the CreateNotebookInstanceLifecycleConfig API	Read	notebook-instance-lifecycle-config* (p. 1679)		
DescribePipeline	Grants permission to get information about a pipeline	Read	pipeline* (p. 1682)		
DescribePipelineExecution	Grants permission to get the pipeline definition for a pipeline execution	Read	pipeline-execution* (p. 1682)		
DescribePipelineExecutionInfo	Grants permission to get information about a pipeline execution	Read	pipeline-execution* (p. 1682)		
DescribeProcessingJob	Grants permission to return information about a processing job	Read	processing-job* (p. 1680)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeProject	Grants permission to describe a project	Read	project* (p. 1680)		
DescribeStudioLifecycleConfiguration	Grants permission to describe a Studio Lifecycle Configuration	Read	studio-lifecycle-config* (p. 1679)		
DescribeSubscribedWorkteamInformation	Grants permission to return information about a subscribed workteam	Read	workteam* (p. 1678)		
DescribeTrainingJobInformation	Grants permission to return information about a training job	Read	training-job* (p. 1680)		
DescribeTransformJobInformation	Grants permission to return information about a transform job	Read	transform-job* (p. 1681)		
DescribeTrial	Grants permission to return information about a trial	Read	experiment-trial* (p. 1682)		
DescribeTrialComponentInformation	Grants permission to return information about a trial component	Read	experiment-trial-component* (p. 1682)		
DescribeUserProfile	Grants permission to describe a UserProfile	Read	user-profile* (p. 1679)		
DescribeWorkforce	Grants permission to return information about a workforce	Read	workforce* (p. 1679)		
DescribeWorkteam	Grants permission to return information about a workteam	Read	workteam* (p. 1678)		
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* (p. 1682)		
			experiment-trial-component* (p. 1682)		
			processing-job* (p. 1680)		
EnableSageMakerServiceCatalogPortfolio	Grants permission to enable a SageMaker Service Catalog Portfolio	Write			
GetDeviceFleetReport	Grants permission to access a summary of the devices in a device fleet	Read	device-fleet* (p. 1678)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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* (p. 1678)		
GetLineageGroup	Grants permission to retrieve a lineage group policy	Read			
GetModelPackage	Grants permission to get a Model Package Group policy	Read	model-package-group* (p. 1680)		
GetRecord	Grants permission to get a record from a feature group	Read	feature-group* (p. 1682)		
GetSagemakerServiceCatalogPortfolio	Grants permission to get a SageMaker Service Catalog Portfolio	Read			
GetSearchSuggestions	Grants permission to get search suggestions when provided with a keyword	Read			
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* (p. 1681)		
				sagemaker:TargetModel (p. 1684)	
InvokeEndpointAsync	Grants permission to get inferences from the hosted model at the specified endpoint in an asynchronous manner	Read	endpoint* (p. 1681)		
ListActions	Grants permission to list actions	List			
ListAlgorithms	Grants permission to list Algorithms	List			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAutoMLJobs	Grants permission to list AutoML jobs	List			
ListCandidatesForCompilationJobs	Grants permission to lists candidates for an AutoML job	List			
ListCodeRepositories	Grants permission to list code repositories	List			
ListCompilationJobs	Grants permission to list compilation jobs	List			
ListContexts	Grants permission to list contexts	List			
ListDataQualityJobDefinitions	Grants permission to list data quality job definitions	List			
ListDeviceFleets	Grants permission to list device fleets	List			
ListDevices	Grants permission to list devices	List			
ListDomains	Grants permission to list the Domains in your account	List			
ListEdgePackagingJobs	Grants permission to list edge packaging jobs	List			
ListEndpointConfigurations	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			
ListHumanLoops	Grants permission to return summary information about human loops, given the specified parameters	List			
ListHumanTaskUiSummary	Grants permission to return summary information about human review workflow user interfaces, given the specified parameters	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListHyperParameters	Grants permission to list hyper parameters for training jobs	List			
ListImageVersions	Grants permission to list ImageVersions that belong to a SageMaker Image	List	image* (p. 1680)		
ListImages	Grants permission to list SageMaker Images in your account	List			
ListInferenceRecommendations	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* (p. 1678)		
ListLineageGroups	Grants permission to list lineage groups	List			
ListModelBiasJobs	Grants permission to list model bias job definitions	List			
ListModelExplainedPredictabilityJobs	Grants permission to list model explained predictability job definitions	List			
ListModelMetadataJobs	Grants permission to list model metadata for inference recommendations jobs	List			
ListModelPackageGroups	Grants permission to list Model Package Groups	List			
ListModelPackages	Grants permission to list Model Packages	List	model-package-group (p. 1680)		
ListModelQualityJobs	Grants permission to list model quality job definitions	List			
ListModels	Grants permission to list the models created with the CreateModel API	List			
ListMonitoringExecutions	Grants permission to list monitoring executions	List			
ListMonitoringSchedules	Grants permission to list monitoring schedules	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListNotebookInstancesLifecycleConfigurations	Grants permission to list the Amazon SageMaker notebook instances in the requester's account in an AWS Region	List			
ListNotebookInstances	Grants permission to list the Amazon SageMaker notebook instances in the requester's account in an AWS Region	List			
ListPipelineExecutionsForSteps	Grants permission to list steps for a pipeline execution	List	pipeline-execution* (p. 1682)		
ListPipelineExecutions	Grants permission to list executions for a pipeline	List	pipeline* (p. 1682)		
ListPipelineParametersForStep	Grants permission to list parameters for a pipeline execution	List	pipeline-execution* (p. 1682)		
ListPipelines	Grants permission to list pipelines	List			
ListProcessingJobs	Grants permission to list processing jobs	List			
ListProjects	Grants permission to list Projects	List			
ListStudioLifecycleConfigurations	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 (p. 1682)		

Service Authorization Reference
 Service Authorization Reference
 Amazon SageMaker

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			data-quality-job-definition (p. 1681)		
			device (p. 1678)		
			device-fleet (p. 1678)		
			domain (p. 1679)		
			edge-packaging-job (p. 1678)		
			endpoint (p. 1681)		
			endpoint-config (p. 1681)		
			experiment (p. 1682)		
			experiment-trial (p. 1682)		
			experiment-trial-component (p. 1682)		
			feature-group (p. 1682)		
			flow-definition (p. 1678)		
			human-task-ui (p. 1678)		
			hyper-parameter-tuning-job (p. 1680)		
			image (p. 1680)		
			labeling-job (p. 1678)		
			model (p. 1680)		
			model-bias-job-definition (p. 1681)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			model-explainability-job-definition (p. 1681)		
			model-package (p. 1680)		
			model-package-group (p. 1680)		
			model-quality-job-definition (p. 1681)		
			monitoring-schedule (p. 1681)		
			notebook-instance (p. 1679)		
			pipeline (p. 1682)		
			project (p. 1680)		
			training-job (p. 1680)		
			transform-job (p. 1681)		
			user-profile (p. 1679)		
			workteam (p. 1678)		
ListTrainingJobs	Grants permission to list training jobs	List			
ListTrainingJobsForHyperParameterTuningJob	Grants permission to list training jobs for a hyperparameter tuning job	List	hyper-parameter-tuning-job* (p. 1680)		
ListTransformJobs	Grants permission to list transform jobs	List			
ListTrialComponents	Grants permission to list trial components	List			
ListTrials	Grants permission to list trials	List			
ListUserProfiles	Grants permission to list the UserProfiles in your account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListWorkforces	Grants permission to list workforces	List			
ListWorkteams	Grants permission to list workteams	List			
PutLineageGroup	Grants permission to put a lineage group policy	Write			
PutModelPackageGroup	Grants permission to put a Model Package Group policy	Write	model-package-group* (p. 1680)		
PutRecord	Grants permission to put a record to a feature group	Write	feature-group* (p. 1682)		
QueryLineage	Grants permission to explore the lineage graph	List			
RegisterDevices	Grants permission to register a set of devices	Write	device* (p. 1678)		
				aws:RequestTag/\${TagKey} (p. 1683)	
				aws:TagKeys (p. 1683)	
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* (p. 1682)		
Search	Grants permission to search for SageMaker objects	Read			
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* (p. 1678)		
SendPipelineExecutionFailureCallback	Grants permission to fail a pending callback step	Write	pipeline-execution* (p. 1682)		
SendPipelineExecutionSuccessCallback	Grants permission to succeed a pending callback step	Write	pipeline-execution* (p. 1682)		
StartHumanLoop	Grants permission to start a human loop	Write	flow-definition* (p. 1678)		
StartMonitoringSchedule	Grants permission to start a monitoring schedule	Write	monitoring-schedule* (p. 1681)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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* (p. 1679)		
StartPipelineExecution	Grants permission to start a pipeline execution	Write	pipeline* (p. 1682)		
StopAutoMLJob	Grants permission to stop a running AutoML job	Write	automl-job* (p. 1681)		
StopCompilationJob	Grants permission to stop a compilation job	Write	compilation-job* (p. 1681)		
StopEdgePackagingJob	Grants permission to stop an edge packaging job	Write	edge-packaging-job* (p. 1678)		
StopHumanLoop	Grants permission to stop a specified human loop	Write	human-loop* (p. 1678)		
StopHyperParameterTuningJob	Grants permission to stop a hyper parameter tuning job create via the CreateHyperParameterTuningJob	Write	hyper-parameter-tuning-job* (p. 1680)		
StopInferenceRecommendationsJob	Grants permission to stop an inference recommendations job	Write	inference-recommendations-job* (p. 1678)		
StopLabelingJob	Grants permission to stop a labeling job. Any labels already generated will be exported before stopping	Write	labeling-job* (p. 1678)		
StopMonitoringSchedule	Grants permission to stop a monitoring schedule	Write	monitoring-schedule* (p. 1681)		
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* (p. 1679)		
StopPipelineExecution	Grants permission to stop a pipeline execution	Write	pipeline-execution* (p. 1682)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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* (p. 1680)		
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* (p. 1680)		
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* (p. 1681)		
UpdateAction	Grants permission to update an action	Write	action* (p. 1682)		
UpdateAppImageConfig	Grants permission to update an AppImageConfig	Write	app-image-config* (p. 1679)		
UpdateArtifact	Grants permission to update an artifact	Write	artifact* (p. 1682)		
UpdateCodeRepository	Grants permission to update a CodeRepository	Write	code-repository* (p. 1679)		
UpdateContext	Grants permission to update a context	Write	context* (p. 1682)		
UpdateDeviceFleet	Grants permission to update a device fleet	Write	device-fleet* (p. 1678)		
UpdateDevices	Grants permission to update a set of devices	Write	device* (p. 1678)		
UpdateDomain	Grants permission to update a Domain	Write	domain* (p. 1679)		
			sagemaker:VpcSecurityGroupIds (p. 1684)	sagemaker:InstanceTypes (p. 1684)	sagemaker:DomainSharingOutputKms
		sagemaker:ImageArns (p. 1683)	sagemaker:ImageVersionArns (p. 1684)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateEndpoint	Grants permission to update an endpoint to use the endpoint configuration specified in the request	Write	endpoint* (p. 1681)		
UpdateEndpointWeightCapacity	Grants permission to update VariantWeightCapacity , or both of one or more variants associated with an endpoint	Write	endpoint* (p. 1681)		
UpdateExperiment	Grants permission to update an experiment	Write	experiment* (p. 1682)		
UpdateImage	Grants permission to update the properties of a SageMaker Image	Write	image* (p. 1680)		iam:PassRole
UpdateModelPackage	Grants permission to update a ModelPackage	Write	model-package* (p. 1680)		sagemaker:ModelApprovalStatus (p. 1684)
UpdateMonitoringSchedule	Grants permission to update a monitoring schedule	Write	monitoring-schedule* (p. 1681)		iam:PassRole aws:RequestTag/\${TagKey} (p. 1683) aws:TagKeys (p. 1683) sagemaker:InstanceTypes (p. 1684) sagemaker:MaxRuntimeInSeconds (p. 1684) sagemaker:NetworkIsolation (p. 1684) sagemaker:OutputKmsKey (p. 1684) sagemaker:VolumeKmsKey (p. 1684) sagemaker:VpcSecurityGroupIds (p. 1684) sagemaker:VpcSubnets (p. 1684) sagemaker:InterContainerTrafficEncryption (p. 1684)
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. You can also update the VPC security groups	Write	notebook-instance* (p. 1679)		sagemaker:AcceleratorTypes (p. 1683) sagemaker:InstanceTypes (p. 1684) sagemaker:RootAccess (p. 1684)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateNotebookInstanceLifecycleConfig	Grants permission to update a <code>notebook-instance-lifecycle-config</code> configuration created with the <code>CreateNotebookInstanceLifecycleConfig</code> API	Write	<code>notebook-instance-lifecycle-config*</code> (p. 1679)		
UpdatePipeline	Grants permission to update a pipeline	Write	<code>pipeline*</code> (p. 1682)		iam:PassRole
UpdatePipelineExecution	Grants permission to update a pipeline execution	Write	<code>pipeline-execution*</code> (p. 1682)		
UpdateProject	Grants permission to update a Project	Write	<code>project*</code> (p. 1680)		
				<code>aws:RequestTag/\${TagKey}</code> (p. 1683)	
				<code>aws:TagKeys</code> (p. 1683)	
UpdateTrainingJob	Grants permission to update a training job	Write	<code>training-job*</code> (p. 1680)		
					<code>sagemaker:InstanceTypes</code> (p. 1684)
UpdateTrial	Grants permission to update a trial	Write	<code>experiment-trial*</code> (p. 1682)		
UpdateTrialComponent	Grants permission to update a trial component	Write	<code>experiment-trial-component*</code> (p. 1682)		
UpdateUserProfile	Grants permission to update a UserProfile	Write	<code>user-profile*</code> (p. 1679)		
				<code>sagemaker:InstanceTypes</code> (p. 1684)	
				<code>sagemaker:VpcSecurityGroupIds</code> (p. 1684)	
				<code>sagemaker:InstanceTypes</code> (p. 1684)	
				<code>sagemaker:DomainSharingOutputKms</code> (p. 1684)	
				<code>sagemaker:ImageArns</code> (p. 1683)	
				<code>sagemaker:ImageVersionArns</code> (p. 1684)	
UpdateWorkforce	Grants permission to update a workforce	Write	<code>workforce*</code> (p. 1679)		
UpdateWorkteam	Grants permission to update a workteam	Write	<code>workteam*</code> (p. 1678)		

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 \(p. 1642\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
device	<code>arn:\${Partition}:sagemaker:\${Region}: \${Account}:device-fleet/\${DeviceFleetName}/ device/\${DeviceName}</code>	<code>aws:ResourceTag/ \${TagKey} (p. 1683)</code> <code>sagemaker:ResourceTag/ \${TagKey} (p. 1684)</code>
device-fleet	<code>arn:\${Partition}:sagemaker:\${Region}: \${Account}:device-fleet/\${DeviceFleetName}</code>	<code>aws:ResourceTag/ \${TagKey} (p. 1683)</code> <code>sagemaker:ResourceTag/ \${TagKey} (p. 1684)</code>
edge-packaging-job	<code>arn:\${Partition}:sagemaker:\${Region}: \${Account}:edge-packaging-job/ \${EdgePackagingJobName}</code>	<code>aws:ResourceTag/ \${TagKey} (p. 1683)</code> <code>sagemaker:ResourceTag/ \${TagKey} (p. 1684)</code>
human-loop	<code>arn:\${Partition}:sagemaker:\${Region}: \${Account}:human-loop/\${HumanLoopName}</code>	
flow-definition	<code>arn:\${Partition}:sagemaker: \${Region}: \${Account}:flow-definition/ \${FlowDefinitionName}</code>	<code>aws:ResourceTag/ \${TagKey} (p. 1683)</code> <code>sagemaker:ResourceTag/ \${TagKey} (p. 1684)</code>
human-task-ui	<code>arn:\${Partition}:sagemaker:\${Region}: \${Account}:human-task-ui/\${HumanTaskUiName}</code>	<code>aws:ResourceTag/ \${TagKey} (p. 1683)</code> <code>sagemaker:ResourceTag/ \${TagKey} (p. 1684)</code>
inference-recommendations-job	<code>arn:\${Partition}:sagemaker:\${Region}: \${Account}:inference-recommendations-job/ \${InferenceRecommendationsJobName}</code>	<code>aws:ResourceTag/ \${TagKey} (p. 1683)</code> <code>sagemaker:ResourceTag/ \${TagKey} (p. 1684)</code>
labeling-job	<code>arn:\${Partition}:sagemaker:\${Region}: \${Account}:labeling-job/\${LabelingJobName}</code>	<code>aws:ResourceTag/ \${TagKey} (p. 1683)</code> <code>sagemaker:ResourceTag/ \${TagKey} (p. 1684)</code>
workteam	<code>arn:\${Partition}:sagemaker:\${Region}: \${Account}:workteam/\${WorkteamName}</code>	<code>aws:ResourceTag/ \${TagKey} (p. 1683)</code>

Service Authorization Reference
Service Authorization Reference
Amazon SageMaker

Resource types	ARN	Condition keys
		sagemaker:ResourceTag/\${TagKey} (p. 1684)
workforce	arn:\${Partition}:sagemaker:\${Region}: \${Account}:workforce/\${WorkforceName}	aws:ResourceTag/\${TagKey} (p. 1683) sagemaker:ResourceTag/\${TagKey} (p. 1684)
domain	arn:\${Partition}:sagemaker:\${Region}: \${Account}:domain/\${DomainId}	aws:ResourceTag/\${TagKey} (p. 1683) sagemaker:ResourceTag/\${TagKey} (p. 1684)
user-profile	arn:\${Partition}:sagemaker:\${Region}: \${Account}:user-profile/\${DomainId}/ \${UserProfileName}	aws:ResourceTag/\${TagKey} (p. 1683) sagemaker:ResourceTag/\${TagKey} (p. 1684)
app	arn:\${Partition}:sagemaker: \${Region}: \${Account}:app/\${DomainId}/ \${UserProfileName}/\${AppType}/\${AppName}	aws:ResourceTag/\${TagKey} (p. 1683) sagemaker:ResourceTag/\${TagKey} (p. 1684)
app-image-config	arn:\${Partition}:sagemaker:\${Region}: \${Account}:app-image-config/ \${AppImageConfigName}	aws:ResourceTag/\${TagKey} (p. 1683) sagemaker:ResourceTag/\${TagKey} (p. 1684)
studio-lifecycle-config	arn:\${Partition}:sagemaker:\${Region}: \${Account}:studio-lifecycle-config/ \${StudioLifecycleConfigName}	aws:ResourceTag/\${TagKey} (p. 1683) sagemaker:ResourceTag/\${TagKey} (p. 1684)
notebook-instance	arn:\${Partition}:sagemaker:\${Region}: \${Account}:notebook-instance/ \${NotebookInstanceName}	aws:ResourceTag/\${TagKey} (p. 1683) sagemaker:ResourceTag/\${TagKey} (p. 1684)
notebook-instance-lifecycle-config	arn:\${Partition}:sagemaker: \${Region}: \${Account}:notebook- instance-lifecycle-config/ \${NotebookInstanceLifecycleConfigName}	
code-repository	arn:\${Partition}:sagemaker: \${Region}: \${Account}:code-repository/ \${CodeRepositoryName}	aws:ResourceTag/\${TagKey} (p. 1683) sagemaker:ResourceTag/\${TagKey} (p. 1684)

Resource types	ARN	Condition keys
image	arn:\${Partition}:sagemaker:\${Region}: \${Account}:image/\${ImageName}	aws:ResourceTag/\${TagKey} (p. 1683) sagemaker:ResourceTag/\${TagKey} (p. 1684)
image-version	arn:\${Partition}:sagemaker:\${Region}: \${Account}:image-version/\${ImageName}/ \${Version}	
algorithm	arn:\${Partition}:sagemaker:\${Region}: \${Account}:algorithm/\${AlgorithmName}	aws:ResourceTag/\${TagKey} (p. 1683) sagemaker:ResourceTag/\${TagKey} (p. 1684)
training-job	arn:\${Partition}:sagemaker:\${Region}: \${Account}:training-job/\${TrainingJobName}	aws:ResourceTag/\${TagKey} (p. 1683) sagemaker:ResourceTag/\${TagKey} (p. 1684)
processing-job	arn:\${Partition}:sagemaker: \${Region}: \${Account}:processing-job/ \${ProcessingJobName}	aws:ResourceTag/\${TagKey} (p. 1683) sagemaker:ResourceTag/\${TagKey} (p. 1684)
hyper-parameter-tuning-job	arn:\${Partition}:sagemaker: \${Region}: \${Account}:hyper-parameter-tuning-job/ \${HyperParameterTuningJobName}	aws:ResourceTag/\${TagKey} (p. 1683) sagemaker:ResourceTag/\${TagKey} (p. 1684)
project	arn:\${Partition}:sagemaker:\${Region}: \${Account}:project/\${ProjectName}	aws:ResourceTag/\${TagKey} (p. 1683) sagemaker:ResourceTag/\${TagKey} (p. 1684)
model-package	arn:\${Partition}:sagemaker:\${Region}: \${Account}:model-package/\${ModelPackageName}	aws:ResourceTag/\${TagKey} (p. 1683) sagemaker:ResourceTag/\${TagKey} (p. 1684)
model-package-group	arn:\${Partition}:sagemaker:\${Region}: \${Account}:model-package-group/ \${ModelPackageGroupName}	aws:ResourceTag/\${TagKey} (p. 1683) sagemaker:ResourceTag/\${TagKey} (p. 1684)
model	arn:\${Partition}:sagemaker:\${Region}: \${Account}:model/\${ModelName}	aws:ResourceTag/\${TagKey} (p. 1683) sagemaker:ResourceTag/\${TagKey} (p. 1684)

Resource types	ARN	Condition keys
endpoint-config	arn:\${Partition}:sagemaker:\${Region}:\${Account}:endpoint-config/\${EndpointConfigName}	aws:ResourceTag/\${TagKey} (p. 1683) sagemaker:ResourceTag/\${TagKey} (p. 1684)
endpoint	arn:\${Partition}:sagemaker:\${Region}:\${Account}:endpoint/\${EndpointName}	aws:ResourceTag/\${TagKey} (p. 1683) sagemaker:ResourceTag/\${TagKey} (p. 1684)
transform-job	arn:\${Partition}:sagemaker:\${Region}:\${Account}:transform-job/\${TransformJobName}	aws:ResourceTag/\${TagKey} (p. 1683) sagemaker:ResourceTag/\${TagKey} (p. 1684)
compilation-job	arn:\${Partition}:sagemaker:\${Region}:\${Account}:compilation-job/\${CompilationJobName}	
automl-job	arn:\${Partition}:sagemaker:\${Region}:\${Account}:automl-job/\${AutoMLJobJobName}	aws:ResourceTag/\${TagKey} (p. 1683) sagemaker:ResourceTag/\${TagKey} (p. 1684)
monitoring-schedule	arn:\${Partition}:sagemaker:\${Region}:\${Account}:monitoring-schedule/\${MonitoringScheduleName}	aws:ResourceTag/\${TagKey} (p. 1683) sagemaker:ResourceTag/\${TagKey} (p. 1684)
data-quality-job-definition	arn:\${Partition}:sagemaker:\${Region}:\${Account}:data-quality-job-definition/\${DataQualityJobDefinitionName}	aws:ResourceTag/\${TagKey} (p. 1683) sagemaker:ResourceTag/\${TagKey} (p. 1684)
model-quality-job-definition	arn:\${Partition}:sagemaker:\${Region}:\${Account}:model-quality-job-definition/\${ModelQualityJobDefinitionName}	aws:ResourceTag/\${TagKey} (p. 1683) sagemaker:ResourceTag/\${TagKey} (p. 1684)
model-bias-job-definition	arn:\${Partition}:sagemaker:\${Region}:\${Account}:model-bias-job-definition/\${ModelBiasJobDefinitionName}	aws:ResourceTag/\${TagKey} (p. 1683) sagemaker:ResourceTag/\${TagKey} (p. 1684)
model-explainability-job-definition	arn:\${Partition}:sagemaker:\${Region}:\${Account}:model-explainability-job-definition/\${ModelExplainabilityJobDefinitionName}	aws:ResourceTag/\${TagKey} (p. 1683) sagemaker:ResourceTag/\${TagKey} (p. 1684)

Resource types	ARN	Condition keys
experiment	arn:\${Partition}:sagemaker:\${Region}: \${Account}:experiment/\${ExperimentName}	aws:ResourceTag/ \${TagKey} (p. 1683) sagemaker:ResourceTag/ \${TagKey} (p. 1684)
experiment-trial	arn:\${Partition}:sagemaker:\${Region}: \${Account}:experiment-trial/\${TrialName}	aws:ResourceTag/ \${TagKey} (p. 1683) sagemaker:ResourceTag/ \${TagKey} (p. 1684)
experiment-trial-component	arn:\${Partition}:sagemaker:\${Region}: \${Account}:experiment-trial-component/ \${TrialComponentName}	aws:ResourceTag/ \${TagKey} (p. 1683) sagemaker:ResourceTag/ \${TagKey} (p. 1684)
feature-group	arn:\${Partition}:sagemaker:\${Region}: \${Account}:feature-group/\${FeatureGroupName}	aws:ResourceTag/ \${TagKey} (p. 1683) sagemaker:ResourceTag/ \${TagKey} (p. 1684)
pipeline	arn:\${Partition}:sagemaker:\${Region}: \${Account}:pipeline/\${PipelineName}	aws:ResourceTag/ \${TagKey} (p. 1683) sagemaker:ResourceTag/ \${TagKey} (p. 1684)
pipeline-execution	arn:\${Partition}:sagemaker:\${Region}: \${Account}:pipeline/\${PipelineName}/ execution/\${RandomString}	
artifact	arn:\${Partition}:sagemaker:\${Region}: \${Account}:artifact/\${HashOfArtifactSource}	aws:ResourceTag/ \${TagKey} (p. 1683) sagemaker:ResourceTag/ \${TagKey} (p. 1684)
context	arn:\${Partition}:sagemaker:\${Region}: \${Account}:context/\${ContextName}	aws:ResourceTag/ \${TagKey} (p. 1683) sagemaker:ResourceTag/ \${TagKey} (p. 1684)
action	arn:\${Partition}:sagemaker:\${Region}: \${Account}:action/\${ActionName}	aws:ResourceTag/ \${TagKey} (p. 1683) sagemaker:ResourceTag/ \${TagKey} (p. 1684)
lineage-group	arn:\${Partition}:sagemaker:\${Region}: \${Account}:lineage-group/\${LineageGroupName}	aws:ResourceTag/ \${TagKey} (p. 1683) sagemaker:ResourceTag/ \${TagKey} (p. 1684)

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 [Available global condition 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:AcceleratorType	Filters access by the list of all accelerator types associated with the resource in the request	ArrayOfString
sagemaker:AppNetworkType	Filters access by the app network access type associated with the resource in the request	String
sagemaker:DirectInternetAccess	Filters access by the direct internet access associated with the resource in the request	String
sagemaker:DomainSharingOutputKmsKey	Filters access by the Domain sharing output KMS key associated with the resource in the request	ARN
sagemaker:FeatureGroupOfflineStoreKmsKey	Filters access by the offline store kms key associated with the feature group resource in the request	ARN
sagemaker:FeatureGroupOfflineStoreS3Uri	Filters access by the offline store s3 uri associated with the feature group resource in the request	String
sagemaker:FeatureGroupOnlineStoreKmsKey	Filters access by the online store kms key associated with the feature group resource in the request	ARN
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:HomeEfsFilesystemVolumeKmsKey	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:ImageArn	Filters access by the list of all image arns associated with the resource in the request	ArrayOfString

Condition keys	Description	Type
<code>sagemaker:ImageVersionWithThe</code>	Filters access by the list of all image version arns associated with the resource in the request	ArrayOfString
<code>sagemaker:InstanceTypeWithThe</code>	Filters access by the list of all instance types associated with the resource in the request	ArrayOfString
<code>sagemaker:InterContainerTrafficEncryptionAssociatedWithThe</code>	Filters access by the inter container traffic encryption associated with the resource in the request	Bool
<code>sagemaker:MaxRuntimeForResource</code>	Filters access by the max runtime in seconds associated with the resource in the request	Numeric
<code>sagemaker:ModelApprovalStatusWithThe</code>	Filters access by the model approval status with the model package in the request	String
<code>sagemaker:ModelArnIn</code>	Filters access by the model arn associated with the resource in the request	ARN
<code>sagemaker:NetworkIsolation</code>	Filters access by the network isolation associated with the resource in the request	Bool
<code>sagemaker:OutputKmsKey</code>	Filters access by the output kms key associated with the resource in the request	ARN
<code>sagemaker:ResourceTag/Tag</code>	Filters access by the preface string for a tag key and value pair attached to a resource	String
<code>sagemaker:ResourceTag/\${TagKey}</code>	Filters access by a tag key and value pair	String
<code>sagemaker:RootAccess</code>	Filters access by the root access associated with the resource in the request	String
<code>sagemaker:ServerlessConcurrency</code>	Filters access by limiting maximum concurrency used for Serverless inference in the request	Numeric
<code>sagemaker:ServerlessMemorySize</code>	Filters access by limiting memory size used for Serverless inference in the request	Numeric
<code>sagemaker:TargetModel</code>	Filters access by the target model associated with the Multi-Model Endpoint in the request	String
<code>sagemaker:VolumeKmsKey</code>	Filters access by the volume kms key associated with the resource in the request	ARN
<code>sagemaker:VpcSecurityGroupsAssociatedWith</code>	Filters access by the list of all VPC security group ids associated with the resource in the request	ArrayOfString
<code>sagemaker:VpcSubnets</code>	Filters access by the list of all VPC subnets associated with the resource in the request	ArrayOfString
<code>sagemaker:WorkteamArn</code>	Filters access by the workteam arn associated to the request	ARN
<code>sagemaker:WorkteamType</code>	Filters access by the workteam type associated to the request. This can be public-crowd, private-crowd or vendor-crowd	String

Actions, resources, and condition keys for AWS Savings Plans

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

References:

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

Topics

- [Actions defined by AWS Savings Plans \(p. 1685\)](#)
- [Resource types defined by AWS Savings Plans \(p. 1686\)](#)
- [Condition keys for AWS Savings Plans \(p. 1686\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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} (p. 1687) aws:TagKeys (p. 1687)	
DeleteQueuedSavingsPlan	Grants permission to delete the <code>queued</code> savings plan associated with customers account	Write	savingsplan* (p. 1686)	aws:ResourceTag/\${TagKey} (p. 1687)	
DescribeSavingsPlan	Grants permission to describe the <code>Rates</code> associated with customers savings plan	Read	savingsplan* (p. 1686)	aws:ResourceTag/\${TagKey} (p. 1687)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeSavingsPlans	Grants permission to describe the savings plans associated with customers account	Read	savingsplan*	(p. 1686)	
				aws:ResourceTag/ {\$TagKey} (p. 1687)	
DescribeOfferings	Grants permission to describe the offerings associated with savings plans offerings	Read			
DescribeOfferingsForCustomer	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*	(p. 1686)	
TagResource	Grants permission to tag a savings plan	Tagging	savingsplan*	(p. 1686)	
				aws:TagKeys (p. 1687)	
UntagResource	Grants permission to untag a savings plan	Tagging	savingsplan*	(p. 1686)	
				aws:TagKeys (p. 1687)	

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 \(p. 1685\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1687)

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 [Available global condition 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	String

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 \(p. 1687\)](#)
- [Resource types defined by AWS Secrets Manager \(p. 1694\)](#)
- [Condition keys for AWS Secrets Manager \(p. 1695\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelRotateSecret	Grants permission to cancel an in-progress secret rotation	Write	Secret* (p. 1694)		

Service Authorization Reference
Service Authorization Reference
AWS Secrets Manager

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					secretsmanager:SecretId (p. 1696) secretsmanager:resource/AllowRotationLambdaArn (p. 1696) secretsmanager:ResourceTag/tag-key (p. 1695) aws:ResourceTag/\${TagKey} (p. 1695) secretsmanager:SecretPrimaryRegion
CreateSecret	Grants permission to create a secret that stores encrypted data that can be queried and rotated	Write	Secret* (p. 1694)		
					secretsmanager:Name (p. 1695) secretsmanager:Description (p. 1695) secretsmanager:KmsKeyId (p. 1695) aws:RequestTag/\${TagKey} (p. 1695) aws:ResourceTag/\${TagKey} (p. 1695) aws:TagKeys (p. 1695) secretsmanager:ResourceTag/tag-key (p. 1695) secretsmanager:AddReplicaRegions (p. 1695) secretsmanager:ForceOverwriteReplica
DeleteResourcePolicy	Grants permission to delete the resource policy attached to a secret	Permissions management	Secret* (p. 1694)		
DeleteSecret	Grants permission to delete a secret	Write	Secret* (p. 1694)		

Service Authorization Reference
 Service Authorization Reference
 AWS Secrets Manager

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					secretsmanager:SecretId (p. 1696) secretsmanager:resource/AllowRotationLambdaArn (p. 1696) secretsmanager:RecoveryWindowInDays secretsmanager:ForceDeleteWithoutRecovery secretsmanager:ResourceTag/tag-key (p. 1695) aws:ResourceTag/\${TagKey} (p. 1695) secretsmanager:SecretPrimaryRegion
DescribeSecret	Grants permission to retrieve the metadata about a secret, but not the encrypted data	Read	Secret* (p. 1694)		
					secretsmanager:SecretId (p. 1696) secretsmanager:resource/AllowRotationLambdaArn (p. 1696) secretsmanager:ResourceTag/tag-key (p. 1695) aws:ResourceTag/\${TagKey} (p. 1695) secretsmanager:SecretPrimaryRegion
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* (p. 1694)		
					secretsmanager:SecretId (p. 1696) secretsmanager:resource/AllowRotationLambdaArn (p. 1696) secretsmanager:ResourceTag/tag-key (p. 1695) aws:ResourceTag/\${TagKey} (p. 1695) secretsmanager:SecretPrimaryRegion
GetSecretValue	Grants permission to retrieve and decrypt the encrypted data	Read	Secret* (p. 1694)		

Service Authorization Reference
 Service Authorization Reference
 AWS Secrets Manager

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					secretsmanager:SecretId (p. 1696) secretsmanager:VersionId (p. 1696) secretsmanager:VersionStage (p. 1696) secretsmanager:resource/AllowRotationLambdaArn (p. 1696) secretsmanager:ResourceTag/tag-key (p. 1695) aws:ResourceTag/\${TagKey} (p. 1695) secretsmanager:SecretPrimaryRegion
ListSecretVersionIds	Grants permission to list the available versions of a secret	Read	Secret* (p. 1694)		
					secretsmanager:SecretId (p. 1696) secretsmanager:resource/AllowRotationLambdaArn (p. 1696) secretsmanager:ResourceTag/tag-key (p. 1695) aws:ResourceTag/\${TagKey} (p. 1695) secretsmanager:SecretPrimaryRegion
ListSecrets	Grants permission to list the available secrets	List			
PutResourcePolicy	Grants permission to attach a resource policy to a secret	Permissions management	Secret* (p. 1694)		
					secretsmanager:SecretId (p. 1696) secretsmanager:resource/AllowRotationLambdaArn (p. 1696) secretsmanager:ResourceTag/tag-key (p. 1695) aws:ResourceTag/\${TagKey} (p. 1695) secretsmanager:BlockPublicPolicy (p. 1695) secretsmanager:SecretPrimaryRegion
PutSecretValue		Write	Secret* (p. 1694)		

Service Authorization Reference
Service Authorization Reference
AWS Secrets Manager

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to create a new version of the secret with new encrypted data			secretsmanager:SecretId (p. 1696) secretsmanager:resource/ AllowRotationLambdaArn (p. 1696) secretsmanager:ResourceTag/ tag- key (p. 1695) aws:ResourceTag/ \${TagKey} (p. 1695) secretsmanager:SecretPrimaryRegion	
RemoveRegionsFromReplication	Grants permission to remove regions from replication	Write	Secret* (p. 1694)		
				secretsmanager:SecretId (p. 1696) secretsmanager:resource/ AllowRotationLambdaArn (p. 1696) secretsmanager:ResourceTag/ tag- key (p. 1695) aws:ResourceTag/ \${TagKey} (p. 1695) secretsmanager:SecretPrimaryRegion	
ReplicateSecretToExisting	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* (p. 1694)		
				secretsmanager:SecretId (p. 1696) secretsmanager:resource/ AllowRotationLambdaArn (p. 1696) secretsmanager:ResourceTag/ tag- key (p. 1695) aws:ResourceTag/ \${TagKey} (p. 1695) secretsmanager:SecretPrimaryRegion secretsmanager:AddReplicaRegions (p. 1695) secretsmanager:ForceOverwriteReplica	
RestoreSecret	Grants permission to cancel deletion of a secret	Write	Secret* (p. 1694)		

Service Authorization Reference
Service Authorization Reference
AWS Secrets Manager

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					secretsmanager:SecretId (p. 1696) secretsmanager:resource/AllowRotationLambdaArn (p. 1696) secretsmanager:ResourceTag/tag-key (p. 1695) aws:ResourceTag/\${TagKey} (p. 1695) secretsmanager:SecretPrimaryRegion
RotateSecret	Grants permission to start rotation of a secret	Write	Secret* (p. 1694)		
					secretsmanager:SecretId (p. 1696) secretsmanager:RotationLambdaARN secretsmanager:resource/AllowRotationLambdaArn (p. 1696) secretsmanager:ResourceTag/tag-key (p. 1695) aws:ResourceTag/\${TagKey} (p. 1695) secretsmanager:SecretPrimaryRegion secretsmanager:ModifyRotationRules secretsmanager:RotateImmediately (p. 1696)
StopReplicationToSecret	Grants permission to remove the secret from replication and promote the secret to a regional secret in the replica Region	Write	Secret* (p. 1694)		
					secretsmanager:SecretId (p. 1696) secretsmanager:resource/AllowRotationLambdaArn (p. 1696) secretsmanager:ResourceTag/tag-key (p. 1695) aws:ResourceTag/\${TagKey} (p. 1695) secretsmanager:SecretPrimaryRegion
TagResource	Grants permission to add tags to a secret	Tagging	Secret* (p. 1694)		

Service Authorization Reference
 Service Authorization Reference
 AWS Secrets Manager

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					secretsmanager:SecretId (p. 1696) aws:RequestTag/\${TagKey} (p. 1695) aws:TagKeys (p. 1695) secretsmanager:resource/AllowRotationLambdaArn (p. 1696) secretsmanager:ResourceTag/tag-key (p. 1695) aws:ResourceTag/\${TagKey} (p. 1695) secretsmanager:SecretPrimaryRegion
UntagResource	Grants permission to remove tags from a secret	Tagging	Secret* (p. 1694)		secretsmanager:SecretId (p. 1696) aws:TagKeys (p. 1695) secretsmanager:resource/AllowRotationLambdaArn (p. 1696) secretsmanager:ResourceTag/tag-key (p. 1695) aws:ResourceTag/\${TagKey} (p. 1695) secretsmanager:SecretPrimaryRegion
UpdateSecret	Grants permission to update a secret with new metadata or with a new version of the encrypted data	Write	Secret* (p. 1694)		secretsmanager:SecretId (p. 1696) secretsmanager:Description (p. 1695) secretsmanager:KmsKeyId (p. 1695) secretsmanager:resource/AllowRotationLambdaArn (p. 1696) secretsmanager:ResourceTag/tag-key (p. 1695) aws:ResourceTag/\${TagKey} (p. 1695) secretsmanager:SecretPrimaryRegion

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateSecretVersionStage	Grants permission to move a stage from one secret to another	Write	Secret* (p. 1694)		
ValidateResourcePolicy	Grants permission to validate a policy before attaching it	Permissions management	Secret* (p. 1694)		

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 \(p. 1687\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1695) aws:ResourceTag/\${TagKey} (p. 1695) aws:TagKeys (p. 1695)

Resource types	ARN	Condition keys
		secretsmanager:ResourceTag/tag-key (p. 1695) secretsmanager:resource/AllowRotationLambdaArn (p. 1696)

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 [Available global condition 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:AddSecretRegions	Filters access by the list of Regions in which to replicate the secret	ArrayOfString
secretsmanager:BlockAWSAccountAccess	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:ForceDeleteWithoutRecovery	Filters access by whether the secret is to be deleted immediately without any recovery window	Bool
secretsmanager:ForceOverwriteSameNameInDestinationRegion	Filters access by whether to overwrite a secret with the same name in the destination Region	Bool
secretsmanager:KmsKeyId	Filters access by the ARN of the KMS key in the request	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:RecoveryWindowBeforeDelete	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

Condition keys	Description	Type
secretsmanager:RotateImmediately	Filters access by whether the secret is to be rotated immediately	Bool
secretsmanager:RotateRequestARN	Filters access by the ARN of the rotation Lambda function in the request	ARN
secretsmanager:SecretId	Filters access by the SecretID value in the request	ARN
secretsmanager:SecretPrimaryRegion	Filters access by primary region in which the secret is created	String
secretsmanager:VersionId	Filters access by the unique identifier of the version of the secret in the request	String
secretsmanager:VersionStage	Filters access by the list of version stages in the request	String
secretsmanager:resourceArn AllowRotationLambdaArn	Filters access by the ARN of the rotation Lambda function associated with the secret	ARN

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 \(p. 1696\)](#)
- [Resource types defined by AWS Security Hub \(p. 1702\)](#)
- [Condition keys for AWS Security Hub \(p. 1702\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 (p. 1702)		
AcceptInvitation	Grants permission to accept Security Hub invitations to become a member account	Write	hub (p. 1702)		
BatchDisableStandards	Grants permission to disable standards in Security Hub	Write	hub (p. 1702)		
BatchEnableStandards	Grants permission to enable standards in Security Hub	Write	hub (p. 1702)		
BatchGetStandardsAssociations [permission only]	Grants permission to get the associations between a list of security controls and standards in batches	Read			
BatchImportFindings	Grants permission to import findings into Security Hub from an integrated product	Write	product* (p. 1702) securityhub:TargetAccount (p. 1703)		
BatchUpdateFindings	Grants permission to update customer-controlled fields for a selected set of Security Hub findings	Write	hub (p. 1702) securityhub:ASFFSyntaxPath/\${ASFFSyntaxPath} (p. 1703)		
BatchUpdateStandardsAssociations [permission only]	Grants permission to update the associations between a list of security controls and standards in batches	Write			
CreateActionTargets	Grants permission to create custom actions in Security Hub	Write	hub (p. 1702)		
CreateFindingAggregators	Grants permission to create 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 (p. 1702)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateMembers	Grants permission to create member accounts in Security Hub	Write	hub (p. 1702)		
DeclineInvitations	Grants permission to decline Security Hub invitations to become a member account	Write	hub (p. 1702)		
DeleteActionTarget	Grants permission to delete custom actions in Security Hub	Write	hub (p. 1702)		
DeleteFindingAggregator	Grants permission to delete a finding aggregator, which disables finding aggregation across Regions	Write	finding-aggregator* (p. 1702)		
DeleteInsight	Grants permission to delete insights from Security Hub	Write	hub (p. 1702)		
DeleteInvitations	Grants permission to delete Security Hub invitations to become a member account	Write	hub (p. 1702)		
DeleteMembers	Grants permission to delete Security Hub member accounts	Write	hub (p. 1702)		
DescribeActionTargets	Grants permission to retrieve a list of custom actions using the API	Read	hub (p. 1702)		
DescribeHub	Grants permission to retrieve information about the hub resource in your account	Read	hub (p. 1702)		
DescribeOrganization	Grants permission to describe the organization configuration for Security Hub	Read	hub (p. 1702)		
DescribeProducts	Grants permission to retrieve information about the available Security Hub product integrations	Read	hub (p. 1702)		
DescribeStandards	Grants permission to retrieve information about Security Hub standards	Read	hub (p. 1702)		
DescribeStandardControls	Grants permission to retrieve information about Security Hub standards controls	Read	hub (p. 1702)		
DisableImportFindings	Grants permission to disable the findings import for a Security Hub integrated product	Write	hub (p. 1702)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableOrganization	Grants permission to remove the Security Hub administrator account for your organization	Write	hub (p. 1702)		organizations:DescribeOrganizations
DisableSecurityHub	Grants permission to disable Security Hub	Write	hub (p. 1702)		
DisassociateFromHub	Grants permission to a Security Hub member account to disassociate from the associated administrator account	Write	hub (p. 1702)		
DisassociateFromHub	Grants permission to a Security Hub master account to disassociate from the associated master account	Write	hub (p. 1702)		
DisassociateMembers	Grants permission to disassociate Security Hub member accounts from the associated administrator account	Write	hub (p. 1702)		
EnableImportFindings	Grants permission to enable the Findings Importing for a Security Hub integrated product	Write	hub (p. 1702)		
EnableOrganization	Grants permission to designate Security Hub administrator account for your organization	Write	hub (p. 1702)		organizations:DescribeOrganizations organizations:EnableAWSOrganizations organizations:RegisterDelegatedAdministrator
EnableSecurityHub	Grants permission to enable Security Hub	Write	hub (p. 1702)		
GetAdhocInsight	Grants permission to retrieve Insight results by providing a set of filters instead of an insight ARN	Read	hub (p. 1702)		
GetAdministrator	Grants permission to retrieve Administrator details about the Security Hub administrator account	Read	hub (p. 1702)		
GetControlFindings	Grants permission to retrieve Control Findings score and counts of finding and control statuses for a security standard	Read	hub (p. 1702)		
GetEnabledStandards	Grants permission to retrieve Enabled Standards list of the standards that are enabled in Security Hub	List	hub (p. 1702)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetFindingAggregators	Grants permission to retrieve details for a finding aggregator, which configures finding aggregation across Regions	Read	finding-aggregator* (p. 1702)		
GetFindings	Grants permission to retrieve a list of findings from Security Hub	Read	hub (p. 1702)		
GetFreeTrialEndDates [permission only]	Grants permission to retrieve the date for an account's free trial of Security Hub	Read	hub (p. 1702)		
GetFreeTrialUsage [permission only]	Grants permission to retrieve information about Security Hub usage during the free trial period	Read	hub (p. 1702)		
GetInsightFindings	Grants permission to retrieve insight finding trend from Security Hub in order to generate a graph	Read	hub (p. 1702)		
GetInsightResults	Grants permission to retrieve insight results from Security Hub	Read	hub (p. 1702)		
GetInsights	Grants permission to retrieve Security Hub insights	List	hub (p. 1702)		
GetInvitationsCount	Grants permission to retrieve the count of Security Hub membership invitations sent to the account	Read	hub (p. 1702)		
GetMasterAccount	Grants permission to retrieve details about the Security Hub master account	Read	hub (p. 1702)		
GetMembers	Grants permission to retrieve the details of Security Hub member accounts	Read	hub (p. 1702)		
GetUsage [permission only]	Grants permission to retrieve information about Security Hub usage by accounts	Read	hub (p. 1702)		
InviteMembers	Grants permission to invite other AWS accounts to become Security Hub member accounts	Write	hub (p. 1702)		
ListControlEvaluations [permission only]	Grants permission to retrieve a list of controls for a standard, including the control IDs, statuses and finding counts	Read	hub (p. 1702)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListEnabledProducts	Grants permission to retrieve the Security Hub integrated products that are currently enabled	List	hub (p. 1702)		
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 (p. 1702)		
ListMembers	Grants permission to retrieve details about Security Hub member accounts associated with the administrator account	List	hub (p. 1702)		
ListOrganizationAdminAccounts	Grants permission to list the Security Hub administrator accounts for your organization	List	hub (p. 1702)		organizations: DescribeOrganization
ListSecurityControlDefinitions [permission only]	Grants permission to retrieve security control definitions, which contain cross-Region control details for security controls	List			
ListTagsForResource	Grants permission to list of tags associated with a resource	Read	hub* (p. 1702)		
SendFindingEvent [permission only]	Grants permission to use a custom action to send Security Hub findings to Amazon EventBridge	Read	hub (p. 1702)		
SendInsightEvent [permission only]	Grants permission to use a custom action to send Security Hub insights to Amazon EventBridge	Read	hub (p. 1702)		
TagResource	Grants permission to add tags to a Security Hub resource	Tagging	hub* (p. 1702)		
UntagResource	Grants permission to remove tags from a Security Hub resource	Tagging	hub* (p. 1702)		
UpdateActionTargets	Grants permission to update custom actions in Security Hub	Write	hub (p. 1702)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateFindingAggregator	Grants permission to update finding aggregator, which contains the cross-Region finding aggregation configuration	Write	finding-aggregator* (p. 1702)		
UpdateFindings	Grants permission to update Security Hub findings	Write	hub (p. 1702)		
UpdateInsight	Grants permission to update insights in Security Hub	Write	hub (p. 1702)		
UpdateOrganizationConfiguration	Grants permission to update the organization configuration for Security Hub	Write	hub (p. 1702)		
UpdateSecurityHubConfiguration	Grants permission to update Security Hub configuration	Write	hub (p. 1702)		
UpdateStandards	Grants permission to update Security Hub standards controls	Write	hub (p. 1702)		

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](#) (p. 1696) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1703)
product	arn:\${Partition}:securityhub:\${Region}: \${Account}:product/\${Company}/#\${ProductId}	
finding-aggregator	arn:\${Partition}:securityhub:\${Region}: \${Account}:finding-aggregator/ \${FindingAggregatorId}	

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters access by actions based on the presence of tag key-value pairs in the request	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters access by actions based on tag key-value pairs attached to the resource	String
<code>aws:TagKeys</code>	Filters access by actions based on the presence of tag keys in the request	ArrayOfString
<code>securityhub:ASFFSyntaxPath/\${ASFFSyntaxPath}</code>	Filters access by the specified fields and values in the request	String
<code>securityhub:TargetAction</code>	Filters access by the AwsAccountId field that is specified in the request	String

Actions, resources, and condition keys for AWS Security Token Service

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

References:

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

Topics

- [Actions defined by AWS Security Token Service \(p. 1703\)](#)
- [Resource types defined by AWS Security Token Service \(p. 1707\)](#)
- [Condition keys for AWS Security Token Service \(p. 1708\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1708)	aws:TagKeys (p. 1708)	aws:PrincipalTag/\${TagKey} (p. 1708)
AssumeRoleWithSAML	Grants permission to obtain a set of temporary security credentials for users who have been authenticated via a SAML authentication response	Write	role* (p. 1708)	saml:namequalifier (p. 1710)	saml:sub (p. 1710)

Service Authorization Reference
 Service Authorization Reference
 AWS Security Token Service

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					saml:edupersonnickname (p. 1709) saml:edupersonorgdn (p. 1709) saml:edupersonorgunitdn (p. 1709) saml:edupersonprimaryaffiliation (p. 1709) saml:edupersonprimaryorgunitdn (p. 1709) saml:edupersonprincipalname (p. 1709) saml:edupersonscopedaffiliation (p. 1709) saml:edupersontargetedid (p. 1710) saml:givenName (p. 1710) saml:mail (p. 1710) saml:name (p. 1710) saml:organizationStatus (p. 1710) saml:primaryGroupSID (p. 1710) saml:surname (p. 1710) saml:uid (p. 1710) saml:x500UniqueIdentifier (p. 1710) aws:TagKeys (p. 1708) aws:PrincipalTag/ \${TagKey} (p. 1708) aws:RequestTag/ \${TagKey} (p. 1708) sts:TransitiveTagKeys (p. 1710) sts:SourceIdentity (p. 1710) sts:RoleSessionName (p. 1710)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssumeRoleWithWebIdentity	Grants permission to obtain temporary security credentials for users who have been authenticated in a mobile or web application with a web identity provider	Write	role* (p. 1708)		
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
GetFederationToken	Grants permission to obtain a set of temporary security credentials (consisting of an access key ID, a secret access key, and a security token) for a federated user	Read	user (p. 1708)		
GetServiceBearerToken	Grants permission to obtain a STS bearer token for an AWS root user, IAM role, or an IAM user	Read			sts:AWSServiceName (p. 1710)
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			
SetSourceIdentity	Grants permission to set a source identity on a STS session	Write	role (p. 1708)		
			user (p. 1708)		sts:SourceIdentity (p. 1710)
					aws:SourceIdentity (p. 1708)
TagSession	Grants permission to add tags to a STS session	Tagging	role (p. 1708)		
			user (p. 1708)		
					aws:TagKeys (p. 1708)
					aws:PrincipalTag/ \${TagKey} (p. 1708)
					aws:RequestTag/ \${TagKey} (p. 1708)
					sts:TransitiveTagKeys (p. 1710)

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 \(p. 1703\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1708)
user	arn:\${Partition}:iam::\${Account}:user/\${UserNameWithPath}	

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 [Available global condition 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
aws:FederatedProviderUser	Filters access by the IdP that was used to authenticate the user	String
aws:PrincipalTag/\${TagKey}	Filters access by the tag associated with the principal that is making 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:SourcelIdentity	Filters access by the source identity that is set on the caller	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	String
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:Cognito	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

Condition keys	Description	Type
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
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
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

Condition keys	Description	Type
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
saml:namequalifier	Filters access by the hash value of the issuer, account ID, and friendly name	String
saml:organizationStatus	Filters access by the organizationStatus attribute	String
saml:primaryGroupSID	Filters access by the primaryGroupSID attribute	String
saml:sub	Filters access by the subject of the claim (the SAML user ID)	String
saml:sub_type	Filters access by the value persistent, transient, or the full Format URI	String
saml:surname	Filters access by the surname attribute	String
saml:uid	Filters access by the uid attribute	String
saml:x500UniqueIdentifier	Filters access by the uid attribute	String
sts:AWSServiceName	Filters access by the service that is obtaining a bearer token	String
sts:ExternalId	Filters access by the unique identifier required when you assume a role in another account	String
sts:RoleSessionName	Filters access by the role session name required when you assume a role	String
sts:SourceIdentity	Filters access by the source identity that is passed in the request	String
sts:TransitiveTagKeys	Filters access by the transitive tag keys that are passed in the request	String
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 \(p. 1711\)](#)
- [Resource types defined by AWS Server Migration Service \(p. 1714\)](#)
- [Condition keys for AWS Server Migration Service \(p. 1714\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAppLaunchConfiguration	Grants permission to delete launch configuration for an existing application	Write			
DeleteAppReplicationConfiguration	Grants permission to delete replication configuration for an existing application	Write			
DeleteAppValidationConfiguration	Grants permission to delete validation configuration for an existing application	Write			
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			
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			
GetAppValidationNotification	Grants permission to get notification sent from application validation script.	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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			
NotifyAppValidation	Grants permission to send notification for application validation script	Write			
PutAppLaunchConfig	Grants permission to create or update launch configuration for an existing application	Write			
PutAppReplicationConfig	Grants permission to create or update replication configuration for an existing application	Write			
PutAppValidationConfig	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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartAppReplication	Grants permission to create and start replication jobs for an existing application	Write			
StartOnDemandAppReplication	Grants permission to start a Replication Job for an existing application	Write			
StartOnDemandReplicationRun	Grants permission to start a Replication Run for an existing replication job	Write			
StopAppReplication	Grants permission to stop and delete replication jobs for an existing application	Write			
TerminateApp	Grants permission to terminate the CloudFormation stack for an existing application	Write			
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 [Available keys for conditions](#).

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.

Topics

- [Actions defined by AWS Serverless Application Repository \(p. 1715\)](#)
- [Resource types defined by AWS Serverless Application Repository \(p. 1716\)](#)
- [Condition keys for AWS Serverless Application Repository \(p. 1716\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
<code>CreateApplication</code>	Creates an application, optionally including an AWS SAM file to create the first application version in the same call.	Write			
<code>CreateApplicationVersion</code>	Creates an application version.	Write	applications* (p. 1716)		
<code>CreateCloudFormationTemplate</code>	Creates an AWS CloudFormation template for the given application.	Write	applications* (p. 1716)		serverlessrepo:applicationType (p. 1716)
<code>CreateCloudFormationTemplate</code>	Creates an AWS CloudFormation template	Write	applications* (p. 1716)		serverlessrepo:applicationType (p. 1716)
<code>DeleteApplication</code>	Deletes the specified application	Write	applications* (p. 1716)		
<code>GetApplication</code>	Gets the specified application.	Read	applications* (p. 1716)		serverlessrepo:applicationType (p. 1716)
<code>GetApplicationPolicy</code>	Gets the policy for the specified application.	Read	applications* (p. 1716)		
<code>GetCloudFormationTemplate</code>	Gets the specified AWS CloudFormation template	Read	applications* (p. 1716)		
<code>ListApplicationDependencies</code>	Retrieves the list of applications containing the application	List	applications* (p. 1716)		serverlessrepo:applicationType (p. 1716)
<code>ListApplicationVersions</code>	Lists versions for the specified application owned by the requester.	List	applications* (p. 1716)		serverlessrepo:applicationType (p. 1716)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListApplications	Lists applications owned by the requester.	List			
PutApplicationPolicy	Puts the policy for the specified application.	Write	applications* (p. 1716)		
SearchApplications	Gets all applications authorized for this user	Read		serverlessrepo:applicationType (p. 1716)	
UnshareApplication	Unshares the specified application	Write	applications* (p. 1716)		
UpdateApplication	Updates meta-data of the application	Write	applications* (p. 1716)		

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 \(p. 1715\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
applications	<code>arn:\${Partition}:serverlessrepo:\${Region}:\${Account}:applications/\${ResourceId}</code>	

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 [Available global condition keys](#).

Condition keys	Description	Type
serverlessrepo:applicationType	Application type	String

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 \(p. 1717\)](#)
- [Resource types defined by AWS Service Catalog \(p. 1726\)](#)
- [Condition keys for AWS Service Catalog \(p. 1727\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1727)		
AssociateAttributeGroup	Grants permission to associate an attribute group with an application	Write	Application* (p. 1726)		
			AttributeGroup* (p. 1726)		
AssociateBudgetWithResource	Grants permission to associate a budget with a resource	Write			
AssociatePrincipalWithPortfolio	Grants permission to associate a principal with a portfolio, giving the specified principal access to any products	Write	Portfolio* (p. 1727)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	associated with the specified portfolio				
AssociateProductWithPortfolio	Grants permission to associate a product with a portfolio	Write			
AssociateResourceWithApplication	Grants permission to associate a resource with an application	Write	Application* (p. 1726)		
AssociateServiceActionWithProvisioningArtifact	Grants permission to associate a service action with a provisioning artifact	Write	Product* (p. 1727)		
AssociateTagOptionWithPortfolio	Grants permission to associate the specified tag option with the specified portfolio or product	Write	Portfolio (p. 1727) Product (p. 1727)		
BatchAssociateServiceActionsWithArtifact	Grants permission to associate multiple service actions with provisioning artifacts	Write			
BatchDisassociateServiceActionsFromArtifact	Grants permission to dissociate a batch of 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* (p. 1726) aws:RequestTag / \${TagKey} (p. 1727) aws:TagKeys (p. 1727)	iam: CreateServiceLinkedRole	
CreateAttributeGroup	Grants permission to create an attribute group		aws:RequestTag / \${TagKey} (p. 1727) aws:TagKeys (p. 1727)		
CreateConstraint	Grants permission to create a constraint on an associated product and portfolio	Write	Product* (p. 1727)		
CreatePortfolio	Grants permission to create a portfolio	Write	Portfolio* (p. 1727) aws:RequestTag / \${TagKey} (p. 1727) aws:TagKeys (p. 1727)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePortfolioShare	Grants permission to share a portfolio you own with another AWS account	Permissions management	Portfolio* (p. 1727)		
CreateProduct	Grants permission to create a product and that product's first provisioning artifact	Write	Product* (p. 1727)		
				aws:RequestTag/ \${TagKey} (p. 1727)	aws:TagKeys (p. 1727)
CreateProvisionedProduct	Grants permission to add a new Provisioned product plan	Write		servicecatalog:accountLevel (p. 1727)	
				servicecatalog:roleLevel (p. 1727)	
				servicecatalog:userLevel (p. 1727)	
CreateProvisioningArtifact	Grants permission to add a provisioning artifact to an existing product	Write	Product* (p. 1727)		
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* (p. 1726)		
DeleteAttributeGroup	Grants permission to delete an attribute group if all associations have been removed from the attribute group	Write	AttributeGroup* (p. 1726)		
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* (p. 1727)		
DeletePortfolioShare	Grants permission to unshare a portfolio you own from an AWS account you previously shared the portfolio with	Permissions management	Portfolio* (p. 1727)		
DeleteProduct	Grants permission to delete a product if all associations have been removed from the product	Write	Product* (p. 1727)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteProvisionedProduct	Grants permission to delete a provisioned product plan	Write		servicecatalog:accountLevel (p. 1727) servicecatalog:roleLevel (p. 1727) servicecatalog:userLevel (p. 1727)	
DeleteProvisioningArtifact	Grants permission to delete a provisioning artifact from a product	Write	Product* (p. 1727)		
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			
DescribePortfolio	Grants permission to describe a portfolio	Read	Portfolio* (p. 1727)		
DescribePortfolioShareStatus	Grants permission to get the status of the specified portfolio share operation	Read			
DescribePortfolioSharesSummary	Grants permission to view a summary of each of the portfolio shares that were created for the specified portfolio	List	Portfolio* (p. 1727)		
DescribeProduct	Grants permission to describe a product as an end-user	Read	Product* (p. 1727)		
DescribeProductAdmin	Grants permission to describe a product as an admin	Read	Product* (p. 1727)		
DescribeProductEndUser	Grants permission to describe a product as an end-user	Read			
DescribeProvisionedProduct	Grants permission to describe a provisioned product	Read		servicecatalog:accountLevel (p. 1727) servicecatalog:roleLevel (p. 1727) servicecatalog:userLevel (p. 1727)	
DescribeProvisionedProductPlan	Grants permission to describe a provisioned product plan	Read		servicecatalog:accountLevel (p. 1727) servicecatalog:roleLevel (p. 1727) servicecatalog:userLevel (p. 1727)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeProvisioningArtifact	Grants permission to describe a provisioning artifact	Read	Product* (p. 1727)		
DescribeProvisioningParameters	Grants permission to describe the parameters that you need to specify to successfully provision a specified provisioning artifact	Read	Product* (p. 1727)		
DescribeRecord	Grants permission to describe a record and lists any outputs	Read			servicecatalog:accountLevel (p. 1727) servicecatalog:roleLevel (p. 1727) servicecatalog:userLevel (p. 1727)
DescribeServiceAction	Grants permission to describe a self-service action	Read			
DescribeServiceActionParameters	Grants permission to get the default parameters if you executed the specified Service Action on the specified Provisioned Product	Read			servicecatalog:accountLevel (p. 1727) servicecatalog:roleLevel (p. 1727) servicecatalog:userLevel (p. 1727)
DescribeTagOption	Grants permission to get information about the specified TagOption	Read			
DisableAWSOrganizationsPortfolioSharing	Grants permission to disable portfolio sharing through AWS Organizations feature	Write			
DisassociateAttributeGroup	Grants permission to disassociate an attribute group from an application	Write	Application* (p. 1726)		
			AttributeGroup* (p. 1726)		
DisassociateBudget	Grants permission to disassociate a budget from a resource	Write			
DisassociatePrincipal	Grants permission to disassociate an IAM principal from a portfolio	Write	Portfolio* (p. 1727)		
DisassociateProduct	Grants permission to disassociate a product from a portfolio	Write			
DisassociateResource	Grants permission to disassociate a resource from an application	Write	Application* (p. 1726)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateServiceArtifact	Grants permission to disassociate the specified service action association from the specified provisioning artifact	Write	Product* (p. 1727)		
DisassociateTagOption	Grants permission to disassociate the specified TagOption from the specified resource	Write	Portfolio (p. 1727)		
			Product (p. 1727)		
EnableAWSOrganizationSharing	Grants permission to enable portfolio sharing feature through AWS Organizations	Write			
ExecuteProvisionedProductPlan	Grants permission to execute a provisioned product plan	Write		servicecatalog:accountLevel (p. 1727) servicecatalog:roleLevel (p. 1727) servicecatalog:userLevel (p. 1727)	
ExecuteProvisionedProductPlan	Grants permission to executes a provisioned product plan	Write		servicecatalog:accountLevel (p. 1727) servicecatalog:roleLevel (p. 1727) servicecatalog:userLevel (p. 1727)	
GetAWSOrganizationSharingAccessStatus	Grants permission to get the access status of AWS Organization portfolio share feature	Read			
GetApplication	Grants permission to get an application	Read	Application* (p. 1726)		
GetAssociatedResourceInformation	Grants permission to get information about a resource associated to an application	Read	Application* (p. 1726)		
GetAttributeGroup	Grants permission to get an attribute group	Read	AttributeGroup* (p. 1726)		
GetProvisionedProductOutput	Grants permission to get the provisioned product output with either provisioned product id or name	Read			
ImportAsProvisionedProductSource	Grants permission to import a resource into a provisioned product	Write	Product* (p. 1727)		
ListAcceptedPortfolios	Grants permission to list the portfolios that have been shared with you and you have accepted	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListApplications	Grants permission to list the applications in your account	List			
ListAssociatedAttributeGroups	Grants permission to list the attribute groups associated with an application	List	Application* (p. 1726)		
ListAssociatedResources	Grants permission to list the resources associated with an application	List	Application* (p. 1726)		
ListAttributeGroups	Grants permission to list the attribute groups in your account	List			
ListBudgetsForResource	Grants permission to list all the budgets associated to a resource	List			
ListConstraintsForPortfolio	Grants permission to list the constraints associated with a given portfolio	List			
ListLaunchPaths	Grants permission to list the different ways to launch a given product as an end-user	List	Product* (p. 1727)		
ListOrganizationPortfolios	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* (p. 1727)		
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* (p. 1727)		
ListPrincipalsForPortfolio	Grants permission to list the IAM principals associated with a given portfolio	List	Portfolio* (p. 1727)		
ListProvisionedProducts	Grants permission to list the provisioned product plans	List		servicecatalog:accountLevel (p. 1727)	
ListProvisioningArtifacts	Grants permission to list the provisioning artifacts associated with a given product	List	Product* (p. 1727)	servicecatalog:roleLevel (p. 1727)	
ListProvisioningArtifacts	Grants permission to list the provisioning artifacts associated with a given product	List	Product* (p. 1727)	servicecatalog:userLevel (p. 1727)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListProvisioningArtifacts	Grants permission to list all provisioning artifacts for the specified self-service action	List			
ListRecordHistory	Grants permission to list all the records in your account or all the records related to a given provisioned product	List		servicecatalog:accountLevel (p. 1727) servicecatalog:roleLevel (p. 1727) servicecatalog:userLevel (p. 1727)	
ListResourcesForTagOption	Grants permission to list the resources associated with the specified TagOption	List			
ListServiceActions	Grants permission to list all self-service actions	List			
ListServiceActionAssocs	Grants permission to list all the service action assocs associated with the specified provisioning artifact in your account	List	Product* (p. 1727)	servicecatalog:accountLevel (p. 1727) servicecatalog:roleLevel (p. 1727) servicecatalog:userLevel (p. 1727)	
ListStackInstances	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 (p. 1727) servicecatalog:roleLevel (p. 1727) servicecatalog:userLevel (p. 1727)	
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 (p. 1726)	AttributeGroup (p. 1726)	
ProvisionProduct	Grants permission to provision a product with a specified provisioning artifact and launch parameters	Write	Product* (p. 1727)		
RejectPortfolioShare	Grants permission to reject a portfolio that has been shared with you that you previously accepted	Write	Portfolio* (p. 1727)		
ScanProvisionedProducts	Grants permission to list all the provisioned products in your account	List		servicecatalog:accountLevel (p. 1727) servicecatalog:roleLevel (p. 1727) servicecatalog:userLevel (p. 1727)	

Service Authorization Reference
Service Authorization Reference
AWS Service Catalog

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SearchProducts	Grants permission to list the products available to you as an end-user	List			
SearchProductsAsOwner	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 (p. 1727)	servicecatalog:roleLevel (p. 1727)
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 (p. 1726)		
			AttributeGroup (p. 1726)		
				aws:TagKeys (p. 1727)	
				aws:RequestTag/ \${TagKey} (p. 1727)	
TerminateProvisionedProduct	Grants permission to terminate an existing provisioned product	Write		servicecatalog:accountLevel (p. 1727)	servicecatalog:roleLevel (p. 1727)
UntagResource	Grants permission to remove a tag from a service catalog appregistry resource	Tagging	Application (p. 1726)		
			AttributeGroup (p. 1726)		
				aws:TagKeys (p. 1727)	
				aws:RequestTag/ \${TagKey} (p. 1727)	
UpdateApplication	Grants permission to update the attributes of an existing application	Write	Application* (p. 1726)		iam>CreateServiceLinkedRole
UpdateAttributeGroup	Grants permission to update the attributes of an existing attribute group	Write	AttributeGroup* (p. 1726)		
UpdateConstraint	Grants permission to update the metadata fields of an existing constraint	Write			
UpdatePortfolio		Write	Portfolio* (p. 1727)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to update the metadata fields and/or tags of an existing portfolio			aws:RequestTag/ \${TagKey} (p. 1727) aws:TagKeys (p. 1727)	
UpdatePortfolioShare	Grants permission to enable or disable resource sharing for an existing portfolio share	Permissions management	Portfolio* (p. 1727)		
UpdateProduct	Grants permission to update the metadata fields and/or tags of an existing product	Write	Product* (p. 1727)		
				aws:RequestTag/ \${TagKey} (p. 1727) aws:TagKeys (p. 1727)	
UpdateProvisionedProduct	Grants permission to update an existing provisioned product	Write		servicecatalog:accountLevel (p. 1727) servicecatalog:roleLevel (p. 1727) servicecatalog:userLevel (p. 1727)	
UpdateProvisionedProperties	Grants permission to update the properties of an existing provisioned product	Write			
UpdateProvisionedMetadata	Grants permission to update the metadata fields of an existing provisioning artifact	Write	Product* (p. 1727)		
UpdateServiceAction	Grants permission to update a self-service action	Write			
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 \(p. 1717\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1727)
AttributeGroup	arn:\${Partition}:servicecatalog: \${Region}://\${Account}:/attribute-groups/ \${AttributeGroupId}	aws:ResourceTag/ \${TagKey} (p. 1727)

Resource types	ARN	Condition keys
Portfolio	arn:\${Partition}:catalog:\${Region}: \${Account}:portfolio/\${PortfolioId}	aws:ResourceTag/ \${TagKey} (p. 1727)
Product	arn:\${Partition}:catalog:\${Region}: \${Account}:product/\${ProductId}	aws:ResourceTag/ \${TagKey} (p. 1727)

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 [Available global condition 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 *AWS 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:accountLevelResources	Filters access by user to see and perform actions on resources created by anyone in the account	String
servicecatalog:roleLevelResources	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
servicecatalog:userLevelResources	Filters access by user to see and perform actions on only resources that they created	String

Actions, resources, and condition keys for Service Quotas

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

References:

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

Topics

- [Actions defined by Service Quotas \(p. 1728\)](#)
- [Resource types defined by Service Quotas \(p. 1730\)](#)
- [Condition keys for Service Quotas \(p. 1730\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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			
DeleteServiceQuotaTemplate	Grants permission to remove the specified service quota from the service quota template	Write			
DisassociateServiceQuotaTemplate	Grants permission to disassociate the Service Quotas template from your organization	Write			
GetAWSDefaultServiceQuotaTemplate	Grants permission to return the details for the specified service quota, including the AWS default value	Read			
GetAssociationForServiceQuotaTemplate	Grants permission to retrieve the <code>ServiceQuotaTemplateAssociationStatus</code> value, which tells you if the Service Quotas template is associated with an organization	Read			
GetRequestedServiceQuotaTemplate	Grants permission to retrieve the details for a particular service quota increase request	Read			
GetServiceQuota	Grants permission to return the details for the specified service	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	quota, including the applied value				
GetServiceQuota	Grants permission to retrieve the details for a service quota increase request from the service quota template	Read			
ListAWSDefaultServiceQuotas	Grants permission to list all default service quotas for the specified AWS service	Read			
ListRequestedServiceQuotas	Grants permission to request a list of the changes to service quotas for a service	Read			
ListRequestedServiceQuotas	Grants permission to request a list of the changes to specific service quotas	Read			
ListServiceQuota	Grants permission to return a list of the service quota increase requests from the service quota template	Read			
ListServiceQuotas	Grants permission to list all service quotas for the specified AWS service, in that account, in that Region	Read			
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			
PutServiceQuota	Grants permission to define and add a Request Tag to the Service Quota template	Write	quota (p. 1730)		
				servicequotas:service (p. 1730)	
RequestServiceQuota	Grants permission to submit the request for a service quota increase	Write	quota (p. 1730)		
				servicequotas:service (p. 1730)	
TagResource	Grants permission to associate a set of tags with an existing SQ resource	Tagging		aws:RequestTag/\${TagKey} (p. 1730)	
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:RequestTag/\${TagKey} (p. 1730)	
				aws:TagKeys (p. 1730)	

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 \(p. 1728\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
quota	<code>arn:\${Partition}:servicequotas:\${Region}:\${Account}: \${ServiceCode}/\${QuotaCode}</code>	

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters access by the tags that are passed in the request	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters access by the tags associated with the resource	String
<code>aws:TagKeys</code>	Filters access by the tag keys that are passed in the request	ArrayOfString
<code>servicequotas:service</code>	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 \(p. 1731\)](#)
- [Resource types defined by Amazon SES \(p. 1737\)](#)
- [Condition keys for Amazon SES \(p. 1738\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CloneReceiptRule	Grants permission to create a receipt rule set by cloning an existing one	Write		ses:ApiVersion (p. 1738)	
CreateConfigurationSet	Grants permission to create a new configuration set	Write		ses:ApiVersion (p. 1738)	
CreateConfigurationSetEventDestination	Grants permission to create a configuration set event destination	Write		ses:ApiVersion (p. 1738)	
CreateConfigurationSetAssociation	Grants permission to creates an association between a configuration set and a custom domain for open and click event tracking	Write		ses:ApiVersion (p. 1738)	
CreateCustomVerificationEmailTemplate	Grants permission to create a new custom verification email template	Write		ses:ApiVersion (p. 1738)	
CreateReceiptFilter	Grants permission to create a new IP address filter	Write		ses:ApiVersion (p. 1738)	
CreateReceiptRule	Grants permission to create a receipt rule	Write		ses:ApiVersion (p. 1738)	
CreateReceiptRuleSet	Grants permission to create an empty receipt rule set	Write		ses:ApiVersion (p. 1738)	
CreateTemplate	Grants permission to creates an email template	Write		ses:ApiVersion (p. 1738)	
DeleteConfigurationSet	Grants permission to delete an existing configuration set	Write		ses:ApiVersion (p. 1738)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteConfigurationEventDestination	Grants permission to delete an event destination	Write		ses:ApiVersion (p. 1738)	
DeleteConfigurationAssociation	Grants permission to delete an association between a configuration set and a custom domain for open and click event tracking	Write		ses:ApiVersion (p. 1738)	
DeleteCustomVerificationEmailTemplate	Grants permission to delete an existing custom verification email template	Write		ses:ApiVersion (p. 1738)	
DeleteIdentity	Grants permission to delete the specified identity	Write		ses:ApiVersion (p. 1738)	
DeleteIdentityPolicy	Grants permission to delete the specified sending authorization policy for the given identity (an email address or a domain)	Permissions management		ses:ApiVersion (p. 1738)	
DeleteReceiptFilter	Grants permission to delete the specified IP address filter	Write		ses:ApiVersion (p. 1738)	
DeleteReceiptRule	Grants permission to delete the specified receipt rule	Write		ses:ApiVersion (p. 1738)	
DeleteReceiptRuleSet	Grants permission to delete the specified receipt rule set and all of the receipt rules it contains	Write		ses:ApiVersion (p. 1738)	
DeleteTemplate	Grants permission to delete an email template	Write		ses:ApiVersion (p. 1738)	
DeleteVerifiedEmailAddress	Grants permission to delete the specified email address from the list of verified addresses	Write		ses:ApiVersion (p. 1738)	
DescribeActiveReceiptRuleSet	Grants permission to return the <code>Metadata</code> and receipt rules for the receipt rule set that is currently active	Read		ses:ApiVersion (p. 1738)	
DescribeConfigurationSet	Grants permission to return the details of the specified configuration set	Read		ses:ApiVersion (p. 1738)	
DescribeReceiptRule	Grants permission to return the details of the specified receipt rule	Read		ses:ApiVersion (p. 1738)	
DescribeReceiptRuleSet	Grants permission to return the details of the specified receipt rule set	Read		ses:ApiVersion (p. 1738)	

Service Authorization Reference
Service Authorization Reference
Amazon SES

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAccountSendingStatistics	Grants permission to return the email sending status of your account	Read		ses:ApiVersion (p. 1738)	
GetCustomVerificationEmailTemplate	Grants permission to return the the custom template verification template for the template name you specify	Read		ses:ApiVersion (p. 1738)	
GetIdentityDkimAttributes	Grants permission to return the the current status of Easy DKIM signing for an entity	Read		ses:ApiVersion (p. 1738)	
GetIdentityMailFromAttributes	Grants permission to return the the custom MAIL FROM attributes for a list of identities (email addresses and/or domains)	Read		ses:ApiVersion (p. 1738)	
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 (p. 1738)	
GetIdentityPolicies	Grants permission to return the requested sending authorization policies for the given identity (an email address or a domain)	Read		ses:ApiVersion (p. 1738)	
GetIdentityVerificationStatus	Grants permission to return the the verification status and (for domain identities) the verification token for a list of identities	Read		ses:ApiVersion (p. 1738)	
GetSendQuota	Grants permission to return the user's current sending limits	Read		ses:ApiVersion (p. 1738)	
GetSendStatistics	Grants permission to returns the user's sending statistics	Read		ses:ApiVersion (p. 1738)	
GetTemplate	Grants permission to return the template object, which includes the subject line, HTML part, and text part for the template you specify	Read		ses:ApiVersion (p. 1738)	
ListConfigurationSets	Grants permission to list all of the configuration sets for your account	List		ses:ApiVersion (p. 1738)	
ListCustomVerificationEmailTemplates	Grants permission to list all of the existing custom verification email templates for your account	List		ses:ApiVersion (p. 1738)	

Service Authorization Reference
Service Authorization Reference
Amazon SES

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListIdentities	Grants permission to list the email identities for your account	List		ses:ApiVersion (p. 1738)	
ListIdentityPolicies	Grants permission to list all of the email templates for your account	List		ses:ApiVersion (p. 1738)	
ListReceiptFilters	Grants permission to list the IP address filters associated with your account	Read		ses:ApiVersion (p. 1738)	
ListReceiptRuleSets	Grants permission to list the receipt rule sets that exist under your account	Read		ses:ApiVersion (p. 1738)	
ListTemplates	Grants permission to list the email templates present in your account	List		ses:ApiVersion (p. 1738)	
ListVerifiedEmailAddresses	Grants permission to list all of the email addresses that have been verified in your account	Read		ses:ApiVersion (p. 1738)	
PutConfigurationSetDeliveryOptions	Grants permission to add or update the delivery options for a configuration set	Write		ses:ApiVersion (p. 1738)	
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 (p. 1738)	
ReorderReceiptRuleSet	Grants permission to reorder the receipt rules within a receipt rule set	Write		ses:ApiVersion (p. 1738)	
SendBounce	Grants permission to generate and send a bounce message to the sender of an email you received through Amazon SES	Write	identity* (p. 1738) ses:ApiVersion (p. 1738) ses:FromAddress (p. 1738)		
SendBulkTemplateEmail	Grants permission to compose and send an email message to multiple destinations			identity* (p. 1738) template* (p. 1738) configuration-set (p. 1738)	

Service Authorization Reference
Service Authorization Reference
Amazon SES

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ses:ApiVersion (p. 1738) ses:FeedbackAddress (p. 1738) ses:FromAddress (p. 1738) ses:FromDisplayName (p. 1738) ses:Recipients (p. 1738)
SendCustomVerificationEmail	Grants permission to add an email address to the list of identities and attempts to verify it for your account	Write	identity* (p. 1738) ses:ApiVersion (p. 1738) ses:FeedbackAddress (p. 1738) ses:FromAddress (p. 1738) ses:FromDisplayName (p. 1738) ses:Recipients (p. 1738)		
SendEmail	Grants permission to send an email message	Write	identity* (p. 1738) configuration-set (p. 1738) ses:ApiVersion (p. 1738) ses:FeedbackAddress (p. 1738) ses:FromAddress (p. 1738) ses:FromDisplayName (p. 1738) ses:Recipients (p. 1738)		
SendRawEmail	Grants permission to send an email message , with header and content specified by the client	Write	identity* (p. 1738) configuration-set (p. 1738) ses:ApiVersion (p. 1738) ses:FeedbackAddress (p. 1738) ses:FromAddress (p. 1738) ses:FromDisplayName (p. 1738) ses:Recipients (p. 1738)		
SendTemplatedEmail	Grants permission to compose an email message using an email template	Write	identity* (p. 1738) template* (p. 1738) configuration-set (p. 1738)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ses:ApiVersion (p. 1738) ses:FeedbackAddress (p. 1738) ses:FromAddress (p. 1738) ses:FromDisplayName (p. 1738) ses:Recipients (p. 1738)
SetActiveReceiptRuleSet	Grants permission to set the specified receipt rule set as the active receipt rule set	Write		ses:ApiVersion (p. 1738)	
SetIdentityDkimEnabled	Grants permission to enable or disable Easy DKIM signing of email sent from an identity	Write		ses:ApiVersion (p. 1738)	
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 (p. 1738)	
SetIdentityHeaderBehavior	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 (p. 1738)	
SetIdentityMailFromDomain	Grants permission to enable or disable the custom MAIL FROM domain setup for a verified identity	Write		ses:ApiVersion (p. 1738)	
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 (p. 1738)	
SetReceiptRulePosition	Grants permission to set the position of the specified receipt rule in the receipt rule set	Write		ses:ApiVersion (p. 1738)	
TestRenderTemplatePreview	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 (p. 1738)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAccountSendEnabled	Grants permission to enable or disable email sending for your account	Write		ses:ApiVersion (p. 1738)	
UpdateConfigurationEventDestination	Grants permission to update the event destination of a configuration set	Write		ses:ApiVersion (p. 1738)	
UpdateConfigurationReputationEnabled	Grants permission to enable or disable the publishingEnabled of reputation metrics for emails sent using a specific configuration set	Write		ses:ApiVersion (p. 1738)	
UpdateConfigurationSendingEnabled	Grants permission to enable or disable email sending for messages sent using a specific configuration set	Write		ses:ApiVersion (p. 1738)	
UpdateConfigurationAssociation	Grants permission to modify the association between a configuration set and a custom domain for open and click event tracking	Write		ses:ApiVersion (p. 1738)	
UpdateCustomVerificationTemplate	Grants permission to update an existing custom verification email template	Write		ses:ApiVersion (p. 1738)	
UpdateReceiptRule	Grants permission to update a receipt rule	Write		ses:ApiVersion (p. 1738)	
UpdateTemplate	Grants permission to update an email template	Write		ses:ApiVersion (p. 1738)	
VerifyDomainDkim	Grants permission to return a set of DKIM tokens for a domain	Write		ses:ApiVersion (p. 1738)	
VerifyDomainIdentity	Grants permission to verify a domain	Write		ses:ApiVersion (p. 1738)	
VerifyEmailAddress	Grants permission to verify an email address	Write		ses:ApiVersion (p. 1738)	
VerifyEmailIdentity	Grants permission to verify an email identity	Write		ses:ApiVersion (p. 1738)	

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 \(p. 1731\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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}	
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 [Available global condition 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
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 Session Manager Message Gateway Service

Amazon Session Manager 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](#).
- Learn how to secure this service and its resources by [using IAM permission policies](#).

Topics

- [Actions defined by Amazon Session Manager Message Gateway Service \(p. 1739\)](#)
- [Resource types defined by Amazon Session Manager Message Gateway Service \(p. 1740\)](#)
- [Condition keys for Amazon Session Manager Message Gateway Service \(p. 1740\)](#)

Actions defined by Amazon Session Manager 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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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			
CreateDataChannel	Grants permission to register a data channel for an instance to send data messages to Systems Manager service	Write			
OpenControlChannel	Grants permission to open a websocket connection for a registered control channel stream from an instance to Systems Manager service	Write			
OpenDataChannel	Grants permission to open a websocket connection for a registered data channel stream from an instance to Systems Manager service	Write			

Resource types defined by Amazon Session Manager Message Gateway Service

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

Condition keys for Amazon Session Manager Message Gateway Service

SSM Messages 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 [Available keys for conditions](#).

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 \(p. 1740\)](#)
- [Resource types defined by AWS Shield \(p. 1744\)](#)
- [Condition keys for AWS Shield \(p. 1744\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateDRTLogBucket	Grants permission to authorize the DDoS Response team to access the specified Amazon S3 bucket containing your flow logs	Write			s3:GetBucketPolicy s3:PutBucketPolicy
AssociateDRTRole	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>ListAttachedRolePoli iam:PassRole
AssociateHealthCheck	Grants permission to add health-based detection to the Shield Advanced protection for a resource	Write	protection* (p. 1744)		route53:GetHealthCheck
				aws:ResourceTag/ \${TagKey} (p. 1745)	
AssociateProactiveEngagement	Grants permission to initialize proactive engagement and set the list of contacts for the DDoS Response Team (DRT) to use	Write			
CreateProtection	Grants permission to activate DDoS protection service for a given resource ARN	Write		aws:RequestTag/ \${TagKey} (p. 1745) aws:TagKeys (p. 1745)	
CreateProtectionGroup	Grants permission to create a group of protected resources so they can be handled as a collective	Write		aws:RequestTag/ \${TagKey} (p. 1745) aws:TagKeys (p. 1745)	
CreateSubscription	Grants permission to activate subscription	Write			
DeleteProtection	Grants permission to delete an existing protection	Write	protection* (p. 1744)		
				aws:ResourceTag/ \${TagKey} (p. 1745)	
DeleteProtectionGroup	Grants permission to remove the specified protection group	Write	protection-group* (p. 1744)		
				aws:ResourceTag/ \${TagKey} (p. 1745)	
DeleteSubscription	Grants permission to deactivate subscription	Write			
DescribeAttack	Grants permission to get attack details	Read	attack* (p. 1744)		
DescribeAttackStatistic	Grants permission to describe information about the number	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	and type of attacks AWS Shield has detected in the last year				
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			
DescribeEmergencyContactDetails	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* (p. 1744)		
				aws:ResourceTag/\${TagKey} (p. 1745)	
DescribeProtectionGroup	Grants permission to describe the specification for the specified protection group	Read	protection-group* (p. 1744)		
					aws:ResourceTag/\${TagKey} (p. 1745)
DescribeSubscription	Grants permission to get subscription details, such as start time	Read			
DisableApplicationLayerAutomatic	Grants permission to disable application layer automatic response for Shield Advanced protection for a resource	Write			
DisableProactiveEscalationAuthorization	Grants permission to remove proactive escalation authorization from the DDoS Response Team (DRT) to notify contacts about escalations	Write			
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
DisassociateDRT	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* (p. 1744)		
					aws:ResourceTag/\${TagKey} (p. 1745)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions	
EnableApplicationLayerAutomaticResponse	Grants permission to enable automatic response for Shield Advanced protection for a resource	Write			cloudfront:GetDistribution iam:CreateServiceLinkedRole iam:GetRole	
EnableProactiveDDoSResponse	Grants permission to authorize the DDoS Response Team (DRT) to use email and phone to notify contacts about escalations	Write				
GetSubscriptionState	Grants permission to get subscription state	Read				
ListAttacks	Grants permission to list all existing attacks	List				
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* (p. 1744)			
ListTagsForResource	Grants permission to get information about AWS tags for a specified Amazon Resource Name (ARN) in AWS Shield	Read	protection (p. 1744)			
				protection-group (p. 1744)		
TagResource	Grants permission to add or updates tags for a resource in AWS Shield		Tagging	protection (p. 1744)		
				protection-group (p. 1744)		
				aws:RequestTag/ \${TagKey} (p. 1745)		
UntagResource	Grants permission to remove tags from a resource in AWS Shield	Tagging	aws:TagKeys (p. 1745)			
				aws:RequestTag/ \${TagKey} (p. 1745)		
				aws:TagKeys (p. 1745)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateApplicationLayerAutomaticResponse	Grants permission to update the details of the automatic response for Shield Advanced protection for a resource	Write			
UpdateEmergencyContactDetails	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* (p. 1744)		
				aws:ResourceTag/\${TagKey} (p. 1745)	
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 \(p. 1740\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1745)
protection-group	arn:\${Partition}:shield::\${Account}:protection-group/\${Id}	aws:ResourceTag/\${TagKey} (p. 1745)

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 [Available global condition 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 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 \(p. 1745\)](#)
- [Resource types defined by AWS Signer \(p. 1747\)](#)
- [Condition keys for AWS Signer \(p. 1747\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddProfilePermissions	Grants permission to add cross-account permissions to a Signing Profile	Permissions management	signing-profile* (p. 1747)		signer:ProfileVersion (p. 1748)

Service Authorization Reference
Service Authorization Reference
AWS Signer

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelSigningProfile	Grants permission to change the state of a Signing Profile to CANCELED	Write	signing-profile* (p. 1747)		
			signer:ProfileVersion (p. 1748)		
DescribeSigningJob	Grants permission to return information about a specific Signing Job	Read	signing-job* (p. 1747)		
GetSigningPlatform	Grants permission to return information about a specific Signing Platform	Read			
GetSigningProfile	Grants permission to return information about a specific Signing Profile	Read	signing-profile* (p. 1747)		
			signer:ProfileVersion (p. 1748)		
ListProfilePermissions	Grants permission to list the cross-account permissions associated with a Signing Profile	Read	signing-profile* (p. 1747)		
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* (p. 1747)		
PutSigningProfile	Grants permission to create a new Signing Profile	Write		aws:RequestTag/\${TagKey} (p. 1747)	
				aws:TagKeys (p. 1748)	
RemoveProfilePermissions	Grants permission to remove cross-account permissions from a Signing Profile	Permissions management	signing-profile* (p. 1747)		
			signer:ProfileVersion (p. 1748)		
RevokeSignature	Grants permission to change the state of a Signing Job to REVOKED	Write	signing-job* (p. 1747)		
			signer:ProfileVersion (p. 1748)		
RevokeSigningProfile	Grants permission to change the state of a Signing Profile to REVOKED	Write	signing-profile* (p. 1747)		
			signer:ProfileVersion (p. 1748)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartSigningJob	Grants permission to initiate a Signing Job on the provided code	Write	signing-profile* (p. 1747)		
					signer:ProfileVersion (p. 1748)
TagResource	Grants permission to add one or more tags to a Signing Profile	Tagging	signing-profile* (p. 1747)		
					aws:TagKeys (p. 1748)
					aws:RequestTag/\${TagKey} (p. 1747)
UntagResource	Grants permission to remove one or more tags from a Signing Profile	Tagging	signing-profile* (p. 1747)		
					aws:TagKeys (p. 1748)
					aws:RequestTag/\${TagKey} (p. 1747)

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 \(p. 1745\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1748)
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 [Available global condition keys](#).

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

Condition keys	Description	Type
aws:ResourceTag/\${TagKey}	Filters access by tag-value associated with the resource	String
aws:TagKeys	Filters access by presence of mandatory tags in the request	ArrayOfString
signer:ProfileVersion	Filters access by version of the Signing Profile	String

Actions, resources, and condition keys for Amazon Simple 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 \(p. 1748\)](#)
- [Resource types defined by Amazon Simple Email Service v2 \(p. 1759\)](#)
- [Condition keys for Amazon Simple Email Service v2 \(p. 1760\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 new configuration set	Write	configuration-set* (p. 1759)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion (p. 1760) aws:TagKeys (p. 1760) aws:RequestTag/\${TagKey} (p. 1760)	
CreateConfigurationSetEventDestination	Grants permission to create a configuration set event destination	Write	configuration-set* (p. 1759)		
			ses:ApiVersion (p. 1760) aws:ResourceTag/\${TagKey} (p. 1760)		
CreateContact	Grants permission to create a contact	Write	contact-list* (p. 1759)		
			ses:ApiVersion (p. 1760) aws:ResourceTag/\${TagKey} (p. 1760)		
CreateContactList	Grants permission to create a contact list	Write	contact-list* (p. 1759)		
			ses:ApiVersion (p. 1760) aws:TagKeys (p. 1760) aws:RequestTag/\${TagKey} (p. 1760)		
CreateCustomVerificationEmailTemplate	Grants permission to create a custom verification email template	Write	custom-verification-email-template* (p. 1759)		
			ses:ApiVersion (p. 1760)		
CreateDedicatedIpPool	Grants permission to create a pool of dedicated IP addresses	Write	dedicated-ip-pool* (p. 1759)		
			ses:ApiVersion (p. 1760) aws:TagKeys (p. 1760) aws:RequestTag/\${TagKey} (p. 1760)		
CreateDeliverabilityTestReport		Write	identity* (p. 1759)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to create a new predictive inbox placement test			ses:ApiVersion (p. 1760) aws:TagKeys (p. 1760) aws:RequestTag/\${TagKey} (p. 1760)	
CreateEmailIdentity	Grants permission to start the process of verifying an email identity	Write	identity* (p. 1759)	ses:ApiVersion (p. 1760) aws:TagKeys (p. 1760) aws:RequestTag/\${TagKey} (p. 1760)	
CreateEmailIdentitySpecified	Grants permission to create the specified sending authorization policy for the given identity	Permissions management	identity* (p. 1759)	ses:ApiVersion (p. 1760) aws:ResourceTag/\${TagKey} (p. 1760)	
CreateEmailTemplate	Grants permission to create an email template	Write	template* (p. 1759)	ses:ApiVersion (p. 1760)	
CreateImportJob	Grants permission to creates an import job for a data destination	Write		ses:ApiVersion (p. 1760)	
DeleteConfigurationSet	Grants permission to delete an existing configuration set	Write	configuration-set* (p. 1759)	ses:ApiVersion (p. 1760) aws:ResourceTag/\${TagKey} (p. 1760)	
DeleteConfigurationSetDestination	Grants permission to delete an event destination	Write	configuration-set* (p. 1759)	ses:ApiVersion (p. 1760) aws:ResourceTag/\${TagKey} (p. 1760)	
DeleteContact	Grants permission to delete a contact from a contact list	Write	contact-list* (p. 1759)	ses:ApiVersion (p. 1760) aws:ResourceTag/\${TagKey} (p. 1760)	
DeleteContactList	Grants permission to delete a contact list with all of its contacts	Write	contact-list* (p. 1759)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion (p. 1760) aws:ResourceTag/\${TagKey} (p. 1760)	
DeleteCustomVerificationEmailTemplate	Grants permission to delete an existing custom verification email template	Write	custom-verification-email-template* (p. 1759)		
				ses:ApiVersion (p. 1760)	
DeleteDedicatedIpPool	Grants permission to delete a dedicated IP pool	Write	dedicated-ip-pool* (p. 1759)		
				ses:ApiVersion (p. 1760) aws:ResourceTag/\${TagKey} (p. 1760)	
DeleteEmailIdentity	Grants permission to delete an email identity	Write	identity* (p. 1759)		
				ses:ApiVersion (p. 1760) aws:ResourceTag/\${TagKey} (p. 1760)	
DeleteEmailIdentityPolicy	Grants permission to delete the specified sending authorization policy for the given identity (an email address or a domain)	Permissions management	identity* (p. 1759)		
				ses:ApiVersion (p. 1760) aws:ResourceTag/\${TagKey} (p. 1760)	
DeleteEmailTemplate	Grants permission to delete an email template	Write	template* (p. 1759)		
				ses:ApiVersion (p. 1760)	
DeleteSuppressedEmailAddress	Grants permission to remove a specific email address from the suppression list for your account	Write		ses:ApiVersion (p. 1760)	
GetAccount	Grants permission to get information about the email-sending status and capabilities for your account	Read		ses:ApiVersion (p. 1760)	
GetBlacklistReport	Grants permission to retrieve a list of the deny lists on which your dedicated IP addresses or tracked domains appear	Read		ses:ApiVersion (p. 1760)	
GetConfigurationSet	Grants permission to get information about an existing configuration set	Read	configuration-set* (p. 1759)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion (p. 1760) aws:ResourceTag/ {\$TagKey} (p. 1760)	
GetConfigurationSets	Grants permission to retrieve destinations that are associated with a configuration set	Read	configuration-set* (p. 1759)		
	ses:ApiVersion (p. 1760) aws:ResourceTag/ {\$TagKey} (p. 1760)				
GetContact	Grants permission to return a contact from a contact list	Read	contact-list* (p. 1759)		
	ses:ApiVersion (p. 1760) aws:ResourceTag/ {\$TagKey} (p. 1760)				
GetContactList	Grants permission to return contact list metadata	Read	contact-list* (p. 1759)		
	ses:ApiVersion (p. 1760)				
GetCustomVerificationTemplate	Grants permission to return verification template for the template name you specify	Read	custom-verification-email-template* (p. 1759)		
	ses:ApiVersion (p. 1760)				
GetDedicatedIp	Grants permission to get information about a dedicated IP address	Read		ses:ApiVersion (p. 1760)	
GetDedicatedIps	Grants permission to list the dedicated IP addresses a dedicated IP pool	Read	dedicated-ip-pool* (p. 1759)		
	ses:ApiVersion (p. 1760) aws:ResourceTag/ {\$TagKey} (p. 1760)				
GetDeliverabilityDashboard	Grants permission to get the Status of the Deliverability dashboard	Read		ses:ApiVersion (p. 1760)	
GetDeliverabilityTestReport	Grants permission to retrieve The Results of a predictive inbox placement test	Read	deliverability-test-report* (p. 1759)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion (p. 1760) aws:ResourceTag/ {\$TagKey} (p. 1760)	
GetDomainDeliverabilityReport	Grants permission to retrieve all the deliverability data for a specific campaign	Read		ses:ApiVersion (p. 1760)	
GetDomainStatistics	Grants permission to retrieve inbox placement and engagement rates for the domains that you use to send email	Read	identity* (p. 1759) ses:ApiVersion (p. 1760) aws:ResourceTag/ {\$TagKey} (p. 1760)		
GetEmailIdentity	Grants permission to get information about a specific identity	Read	identity* (p. 1759) ses:ApiVersion (p. 1760) aws:ResourceTag/ {\$TagKey} (p. 1760)		
GetEmailIdentityRequest	Grants permission to return the requested sending authorization policies for the given identity (an email address or a domain)	Read	identity* (p. 1759) ses:ApiVersion (p. 1760) aws:ResourceTag/ {\$TagKey} (p. 1760)		
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* (p. 1759) ses:ApiVersion (p. 1760)		
GetImportJob	Grants permission to provide information about an import job	Read	import-job* (p. 1759) ses:ApiVersion (p. 1760)		
GetSuppressedDomainInformation	Grants permission to retrieve information about a specific email address that's on the suppression list for your account	Read		ses:ApiVersion (p. 1760)	
ListConfigurationSets	Grants permission to list all of the configuration sets for your account	List		ses:ApiVersion (p. 1760)	
ListContactLists	Grants permission to list all of the contact lists available for your account	List		ses:ApiVersion (p. 1760)	
ListContacts	Grants permission to list the contacts present in a specific contact list	List	contact-list* (p. 1759)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ses:ApiVersion (p. 1760)
ListCustomVerificationEmailTemplates	Grants permission to list all of the existing custom verification email templates for your account	List			ses:ApiVersion (p. 1760)
ListDedicatedIpPools	Grants permission to list all of the dedicated IP pools for your account	List			ses:ApiVersion (p. 1760)
ListDeliverabilityTests	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 (p. 1760)
ListDomainDeliverabilityData	Grants permission to list deliverability data for campaigns that used a specific domain to send email during a specified time range	Read			ses:ApiVersion (p. 1760)
ListEmailIdentities	Grants permission to list the email identities for your account	List			ses:ApiVersion (p. 1760)
ListEmailTemplates	Grants permission to list all of the email templates for your account	List			ses:ApiVersion (p. 1760)
ListImportJobs	Grants permission to list all of the import jobs for your account	List			ses:ApiVersion (p. 1760)
ListSuppressedDestAddresses	Grants permission to list email addresses that are on the suppression list for your account	Read			ses:ApiVersion (p. 1760)
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 (p. 1759)		
contact-list (p. 1759)					
dedicated-ip-pool (p. 1759)					
deliverability-test-report (p. 1759)					
identity (p. 1759)					
			ses:ApiVersion (p. 1760)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutAccountDedicatedIp暖化	Grants permission to enable or disable the automatic warm-up feature for dedicated IP addresses	Write		ses:ApiVersion (p. 1760)	
PutAccountDetails	Grants permission to update your account details	Write		ses:ApiVersion (p. 1760)	
PutAccountSendingDetails	Grants permission to enable or disable the ability to send email for your account	Write		ses:ApiVersion (p. 1760)	
PutAccountSuppressionSettings	Grants permission to change the settings for the account-level suppression list	Write		ses:ApiVersion (p. 1760)	
PutConfigurationSet	Grants permission to associate a configuration set with a dedicated IP pool	Write	configuration-set* (p. 1759)		
				ses:ApiVersion (p. 1760)	aws:ResourceTag/\${TagKey} (p. 1760)
PutConfigurationSetReputation	Grants permission to enable or disable collection of reputation metrics for emails that you send using a particular configuration set	Write	configuration-set* (p. 1759)		
				ses:ApiVersion (p. 1760)	aws:ResourceTag/\${TagKey} (p. 1760)
PutConfigurationSetDelivery	Grants permission to enable or disable email sending for messages that use a particular configuration set	Write	configuration-set* (p. 1759)		
				ses:ApiVersion (p. 1760)	aws:ResourceTag/\${TagKey} (p. 1760)
PutConfigurationSetSuppression	Grants permission to specify the account suppression list preferences for a particular configuration set	Write	configuration-set* (p. 1759)		
				ses:ApiVersion (p. 1760)	aws:ResourceTag/\${TagKey} (p. 1760)
PutConfigurationSetCustomDomain	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* (p. 1759)		
				ses:ApiVersion (p. 1760)	aws:ResourceTag/\${TagKey} (p. 1760)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutDedicatedIpInPool	Grants permission to move a dedicated IP address to an existing dedicated IP pool	Write	dedicated-ip-pool* (p. 1759)		
			ses:ApiVersion (p. 1760)		
			aws:ResourceTag/\${TagKey} (p. 1760)		
PutDedicatedIpWarmUp	Grants permission to put a dedicated IP warm up attributes	Write		ses:ApiVersion (p. 1760)	
PutDeliverabilityDashboardConfig	Grants permission to enable or disable the Deliverability dashboard	Write		ses:ApiVersion (p. 1760)	
PutEmailIdentityConfigurationSetAssociation	Grants permission to associate a configuration set with an email identity	Write	identity* (p. 1759)		
	configuration-set (p. 1759)				
			ses:ApiVersion (p. 1760)		
PutEmailIdentityDisableDKIMAuthentication	Grants permission to enable or disable DKIM authentication for an email identity	Write	identity* (p. 1759)		
			ses:ApiVersion (p. 1760)		
			aws:ResourceTag/\${TagKey} (p. 1760)		
PutEmailIdentityDisableFeedbackForwarding	Grants permission to enable or disable feedback forwarding for an email identity	Write	identity* (p. 1759)		
			ses:ApiVersion (p. 1760)		
			aws:ResourceTag/\${TagKey} (p. 1760)		
PutEmailIdentityDisableCustomMailFrom	Grants permission to enable or disable the custom MAIL FROM domain configuration for an email identity	Write	identity* (p. 1759)		
			ses:ApiVersion (p. 1760)		
			aws:ResourceTag/\${TagKey} (p. 1760)		
PutSuppressedDestination	Grants permission to add an email address to the suppression list	Write		ses:ApiVersion (p. 1760)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendBulkEmail	Grants permission to compose an email message to multiple destinations	Write	identity* (p. 1759) template* (p. 1759) configuration-set (p. 1759)		
			ses:ApiVersion (p. 1760)		
			custom-verification-email-template* (p. 1759)		
			ses:ApiVersion (p. 1760)		
SendEmail	Grants permission to send an email message	Write	identity* (p. 1759) configuration-set (p. 1759) template (p. 1759)		
			ses:ApiVersion (p. 1760) ses:FeedbackAddress (p. 1760) ses:FromAddress (p. 1760) ses:FromDisplayName (p. 1760) ses:Recipients (p. 1760)		
			configuration-set (p. 1759) contact-list (p. 1759)		
			dedicated-ip-pool (p. 1759) deliverability-test-report (p. 1759)		
			identity (p. 1759) ses:ApiVersion (p. 1760) aws:TagKeys (p. 1760) aws:RequestTag/\${TagKey} (p. 1760)		

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* (p. 1759)		
				ses:ApiVersion (p. 1760)	
UntagResource	Grants permission to remove one or more tags (keys and values) from a specified resource	Tagging	configuration-set (p. 1759)		
			contact-list (p. 1759)		
			dedicated-ip-pool (p. 1759)		
			deliverability-test-report (p. 1759)		
			identity (p. 1759)		
				ses:ApiVersion (p. 1760)	
				aws:TagKeys (p. 1760)	
UpdateConfigurationSet	Grants permission to update the configuration of an event destination for a configuration set	Write	configuration-set* (p. 1759)		
				ses:ApiVersion (p. 1760)	
				aws:ResourceTag/\${TagKey} (p. 1760)	
UpdateContact	Grants permission to update a contact's preferences for a list	Write	contact-list* (p. 1759)		
				ses:ApiVersion (p. 1760)	
				aws:ResourceTag/\${TagKey} (p. 1760)	
UpdateContactList	Grants permission to update contact list metadata	Write	contact-list* (p. 1759)		
				ses:ApiVersion (p. 1760)	
				aws:ResourceTag/\${TagKey} (p. 1760)	
UpdateCustomVerificationEmailTemplate	Grants permission to update an existing custom verification email template	Write	custom-verification-email-template* (p. 1759)		
				ses:ApiVersion (p. 1760)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateEmailIdentity	Grants permission to update the sending authorization policy for the given identity (an email address or a domain)	Permissions management	identity* (p. 1759)	ses:ApiVersion (p. 1760) aws:ResourceTag/\${TagKey} (p. 1760)	
UpdateEmailTemplate	Grants permission to update an email template	Write	template* (p. 1759)	ses:ApiVersion (p. 1760)	

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 \(p. 1748\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
configuration-set	<code>arn:\${Partition}:ses:\${Region}: \${Account}:configuration-set/ \${ConfigurationSetName}</code>	aws:ResourceTag/\${TagKey} (p. 1760)
contact-list	<code>arn:\${Partition}:ses:\${Region}: \${Account}:contact-list/ \${ContactListName}</code>	aws:ResourceTag/\${TagKey} (p. 1760)
custom-verification-email-template	<code>arn:\${Partition}:ses:\${Region}: \${Account}:custom-verification-email-template/ \${TemplateName}</code>	
dedicated-ip-pool	<code>arn:\${Partition}:ses:\${Region}: \${Account}:dedicated-ip-pool/ \${DedicatedIPPool}</code>	aws:ResourceTag/\${TagKey} (p. 1760)
deliverability-test-report	<code>arn:\${Partition}:ses:\${Region}: \${Account}:deliverability-test-report/ \${ReportId}</code>	aws:ResourceTag/\${TagKey} (p. 1760)
identity	<code>arn:\${Partition}:ses:\${Region}: \${Account}:identity/ \${IdentityName}</code>	aws:ResourceTag/\${TagKey} (p. 1760)
import-job	<code>arn:\${Partition}:ses:\${Region}: \${Account}:import-job/ \${ImportJobId}</code>	
template	<code>arn:\${Partition}:ses:\${Region}: \${Account}:template/ \${TemplateName}</code>	

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 [Available global condition 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
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 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 \(p. 1761\)](#)
- [Resource types defined by Amazon Simple Workflow Service \(p. 1766\)](#)
- [Condition keys for Amazon Simple Workflow Service \(p. 1767\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelTimer	Grants permission to cancel a previously started timer and record a <code>TimerCanceled</code> event in the history	Write	domain* (p. 1767)		
CancelWorkflowExecution	Grants permission to close the <code>WorkflowExecution</code> and record a <code>WorkflowExecutionCanceled</code> event in the history	Write	domain* (p. 1767)		
CompleteWorkflowExecution	Grants permission to close the <code>WorkflowExecution</code> and record a <code>WorkflowExecutionCompleted</code> event in the history	Write	domain* (p. 1767)		
ContinueAsNewWorkflowExecution	Grants permission to close the <code>WorkflowExecution</code> and start a new workflow execution of the same type using the same workflow ID and a unique run Id	Write	domain* (p. 1767)		
CountClosedWorkflowExecutions	Grants permission to return the number of closed workflow executions within the given domain that meet the specified filtering criteria	Read	domain* (p. 1767)		
				swf:tagFilter.tag (p. 1767)	
				swf:typeFilter.name (p. 1768)	
				swf:typeFilter.version (p. 1768)	
CountOpenWorkflowExecutions	Grants permission to return the number of open workflow executions within the given domain that meet the specified filtering criteria	Read	domain* (p. 1767)		
				swf:tagFilter.tag (p. 1767)	
				swf:typeFilter.name (p. 1768)	
				swf:typeFilter.version (p. 1768)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CountPendingActivityTasks	Grants permission to return the estimated number of activity tasks in the specified task list	Read	domain* (p. 1767)		
			swf:taskList.name (p. 1767)		
CountPendingDecisionTasks	Grants permission to return the estimated number of decision tasks in the specified task list	Read	domain* (p. 1767)		
			swf:taskList.name (p. 1767)		
DeprecateActivityType	Grants permission to deprecate the specified activity type	Write	domain* (p. 1767)		
			swf:activityType.name (p. 1767)		
			swf:activityType.version (p. 1767)		
DeprecateDomain	Grants permission to deprecate the specified domain	Write	domain* (p. 1767)		
DeprecateWorkflowType	Grants permission to deprecate the specified workflow type	Write	domain* (p. 1767)		
			swf:workflowType.name (p. 1768)		
			swf:workflowType.version (p. 1768)		
DescribeActivityType	Grants permission to return information about the specified activity type	Read	domain* (p. 1767)		
			swf:activityType.name (p. 1767)		
			swf:activityType.version (p. 1767)		
DescribeDomain	Grants permission to return information about the specified domain, including its description and status	Read	domain* (p. 1767)		
DescribeWorkflowExecution	Grants permission to return information about the specified workflow execution including its type and some statistics	Read	domain* (p. 1767)		
DescribeWorkflowType	Grants permission to return information about the specified workflow type	Read	domain* (p. 1767)		
			swf:workflowType.name (p. 1768)		
			swf:workflowType.version (p. 1768)		
FailWorkflowExecution	Grants permission to close the workflow execution and record a WorkflowExecutionFailed event in the history	Write	domain* (p. 1767)		
GetWorkflowExecutionHistory	Grants permission to return the history of the specified workflow execution	Read	domain* (p. 1767)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListActivityTypes	Grants permission to return information about all activities registered in the specified domain that match the specified name and registration status	List	domain* (p. 1767)		
ListClosedWorkflowExecutions	Grants permission to return a list of closed workflow executions in the specified domain that meet the filtering criteria	List	domain* (p. 1767)	swf:tagFilter.tag (p. 1767)	
				swf:typeFilter.name (p. 1768)	
				swf:typeFilter.version (p. 1768)	
ListDomains	Grants permission to return the list of domains registered in the account	List			
ListOpenWorkflowExecutions	Grants permission to return a list of open workflow executions in the specified domain that meet the filtering criteria	List	domain* (p. 1767)	swf:tagFilter.tag (p. 1767)	
				swf:typeFilter.name (p. 1768)	
				swf:typeFilter.version (p. 1768)	
ListTagsForResource	Grants permission to list tags for an AWS SWF resource	List	domain (p. 1767)		
ListWorkflowTypes	Grants permission to return information about workflow types in the specified domain	List	domain* (p. 1767)		
PollForActivityTask	Grants permission to workers to get an ActivityTask from the specified activity taskList	Write	domain* (p. 1767)	swf:taskList.name (p. 1767)	
PollForDecisionTask	Grants permission to deciders to get a DecisionTask from the specified decision taskList	Write	domain* (p. 1767)	swf:taskList.name (p. 1767)	
RecordActivityTaskHeartbeat	Grants permission to workers to report to the service that the ActivityTask represented by the specified taskToken is still making progress	Write	domain* (p. 1767)		
RecordMarker	Grants permission to record a MarkerRecorded event in the history	Write	domain* (p. 1767)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterActivityType	Grants permission to register a new activity type along with its configuration settings in the specified domain	Write	domain* (p. 1767)		
RegisterDomain	Grants permission to register a new domain	Write		aws:TagKeys (p. 1767)	aws:RequestTag/\${TagKey} (p. 1767)
RegisterWorkflowType	Grants permission to register a new workflow type and its configuration settings in the specified domain	Write	domain* (p. 1767)		
RequestCancelActivityTask	Grants permission to attempt to cancel a previously scheduled activity task	Write	domain* (p. 1767)		
RequestCancelExternalWorkflowExecution	Grants permission to request that a workflow be canceled	Write	domain* (p. 1767)		
RequestCancelWorkflowExecution	Grants permission to record a <code>WorkflowExecutionCancelRequested</code> event in the currently running workflow execution identified by the given domain, workflowId, and runId	Write	domain* (p. 1767)		
RespondActivityTaskCanceled	Grants permission to workers to tell the service that the ActivityTask identified by the taskToken was successfully canceled	Write	domain* (p. 1767)		

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* (p. 1767)		swf:activityType.name (p. 1767) swf:activityType.version (p. 1767) swf:tagList.member.0 (p. 1767) swf:tagList.member.1 (p. 1767) swf:tagList.member.2 (p. 1767) swf:tagList.member.3 (p. 1767) swf:tagList.member.4 (p. 1767) swf:taskList.name (p. 1767) swf:workflowType.name (p. 1768) swf:workflowType.version (p. 1768)
RespondActivityTaskFailed	Grants permission to workers to tell the service that the ActivityTask identified by the taskToken has failed with reason (if specified)	Write	domain* (p. 1767)		
RespondDecisionTaskCompleted	Grants permission to deciders to tell the service that the DecisionTask identified by the taskToken has successfully completed	Write	domain* (p. 1767)		
ScheduleActivityTask	Grants permission to schedule activity task	Write	domain* (p. 1767)		
SignalExternalWorkflowExecution	Grants permission to request signal to be delivered to the specified external workflow execution and records	Write	domain* (p. 1767)		
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* (p. 1767)		
StartChildWorkflowExecution	Grants permission to request child workflow execution be started	Write	domain* (p. 1767)		
StartTimer	Grants permission to start a timer for a workflow execution	Write	domain* (p. 1767)		

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* (p. 1767)		
				swf:tagList.member.0 (p. 1767)	
				swf:tagList.member.1 (p. 1767)	
				swf:tagList.member.2 (p. 1767)	
				swf:tagList.member.3 (p. 1767)	
				swf:tagList.member.4 (p. 1767)	
				swf:taskList.name (p. 1767)	
				swf:workflowType.name (p. 1768)	
				swf:workflowType.version (p. 1768)	
TagResource	Grants permission to tag an AWS SWF resource	Tagging	domain (p. 1767)		
				aws:TagKeys (p. 1767)	
				aws:RequestTag/\${TagKey} (p. 1767)	
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* (p. 1767)		
UndeprecateActivityType	Grants permission to undeprecate a previously deprecated activity type	Write	domain* (p. 1767)		
				swf:activityType.name (p. 1767)	
				swf:activityType.version (p. 1767)	
UndeprecateDomain	Grants permission to undeprecate a previously deprecated domain	Write	domain* (p. 1767)		
UndeprecateWorkflowType	Grants permission to undeprecate a previously deprecated workflow type	Write	domain* (p. 1767)		
				swf:workflowType.name (p. 1768)	
				swf:workflowType.version (p. 1768)	
UntagResource	Grants permission to remove a tag from an AWS SWF resource	Tagging	domain (p. 1767)		
				aws:TagKeys (p. 1767)	

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 \(p. 1761\)](#) identifies the resource

types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1767)

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 [Available global condition 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
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

Condition keys	Description	Type
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 \(p. 1768\)](#)
- [Resource types defined by Amazon SimpleDB \(p. 1769\)](#)
- [Condition keys for Amazon SimpleDB \(p. 1770\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchDeleteAttributes	Performs multiple DeleteAttributes operations in a single call, which reduces round trips and latencies	Write	domain* (p. 1770)		
BatchPutAttributes	With the BatchPutAttributes operation, you can perform multiple PutAttribute operations in a single call. With the BatchPutAttributes operation, you can perform multiple PutAttribute operations in a single call	Write	domain* (p. 1770)		
CreateDomain	The CreateDomain operation creates a new domain	Write	domain* (p. 1770)		
DeleteAttributes	Deletes one or more attributes associated with the item	Write	domain* (p. 1770)		
DeleteDomain	The DeleteDomain operation deletes a domain	Write	domain* (p. 1770)		
DomainMetadata	Returns 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* (p. 1770)		
GetAttributes	Returns all of the attributes associated with the item	Read	domain* (p. 1770)		
ListDomains	Description for ListDomains	List			
PutAttributes	The PutAttributes operation creates or replaces attributes in an item	Write	domain* (p. 1770)		
Select	Description for Select	Read	domain* (p. 1770)		

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 \(p. 1768\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
domain	arn:\${Partition}:sdb:\${Region}:\${Account}:domain/\${DomainName}	

Condition keys for Amazon SimpleDB

SimpleDB has no service-specific context keys that can be used in the Condition element of policy statements. For the list of the global context keys that are available to all services, see [Available keys for conditions](#).

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 \(p. 1770\)](#)
- [Resource types defined by AWS Snow Device Management \(p. 1772\)](#)
- [Condition keys for AWS Snow Device Management \(p. 1772\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1772)		
CreateTask	Grants permission to create tasks on remote devices	Write		aws:RequestTag/\${TagKey} (p. 1772) aws:TagKeys (p. 1772)	
DescribeDevice	Grants permission to describe a remotely-managed device	Read	managed-device* (p. 1772)		
DescribeDeviceEc2Instances	Grants permission to describe a remotely-managed device's EC2 instances	Read	managed-device* (p. 1772)		
DescribeExecution	Grants permission to describe task executions	Read			
DescribeTask	Grants permission to describe a task	Read	task* (p. 1772)		
ListDeviceResources	Grants permission to list a remotely-managed device's resources	List	managed-device* (p. 1772)		
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} (p. 1772) aws:TagKeys (p. 1772)	
ListTasks	Grants permission to list tasks	List			
TagResource	Grants permission to tag a resource	Tagging	managed-device (p. 1772)		
			task (p. 1772)		
				aws:RequestTag/\${TagKey} (p. 1772) aws:TagKeys (p. 1772)	
UntagResource	Grants permission to untag a resource	Tagging	managed-device (p. 1772)		
			task (p. 1772)		
				aws:RequestTag/\${TagKey} (p. 1772)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					aws:TagKeys (p. 1772)

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 \(p. 1770\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
managed-device	<code>arn:\${Partition}:snow-device-management:\${Region}:\${Account}:managed-device/\${ResourceId}</code>	aws:ResourceTag/\${TagKey} (p. 1772)
task	<code>arn:\${Partition}:snow-device-management:\${Region}:\${Account}:task/\${ResourceId}</code>	aws:ResourceTag/\${TagKey} (p. 1772)

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 [Available global condition keys](#).

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

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](#).

Topics

- [Actions defined by AWS Snowball \(p. 1773\)](#)
- [Resource types defined by AWS Snowball \(p. 1775\)](#)
- [Condition keys for AWS Snowball \(p. 1775\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelCluster	Cancels a cluster job.	Write			
CancelJob	Cancels the specified job.	Write			
CreateAddress	Creates an address for a Snowball to be shipped to.	Write			
CreateCluster	Creates an empty cluster.	Write			
CreateJob	Creates a job to import or export data between Amazon S3 and your on-premises data center.	Write			
CreateLongTermPricingListEntry	Grants permission to creates a LongTermPricingListEntry for allowing customers to add an upfront billing contract for a job	Write			
CreateReturnShippingLabel	Creates a shipping label that will be used to return the Snow device to AWS.	Write			
DescribeAddress	Takes an AddressId and returns specific details about that address in the form of an Address object.	Read			
DescribeAddresses	Returns a specified number of ADDRESS objects.	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeCluster	Returns information about a specific cluster including shipping information, cluster status, and other important metadata.	Read			
DescribeJob	Returns information about a specific job including shipping information, job status, and other important metadata.	Read			
DescribeReturnShipmentLabel	Information on the shipping label of a Snow device that is being returned to AWS.	Read			
GetJobManifest	Returns a link to an Amazon S3 presigned URL for the manifest file associated with the specified JobId value.	Read			
GetJobUnlockCode	Returns the UnlockCode code value for the specified job.	Read			
GetSnowballUsage	Returns information about the Snowball service limit for your account, and also the number of Snowballs your account has in use.	Read			
GetSoftwareUpdate	Returns an Amazon S3 presigned URL for an update file associated with a specified JobId.	Read			
ListClusterJobs	Returns an array of JobListEntry objects of the specified length.	List			
ListClusters	Returns an array of ClusterListEntry objects of the specified length.	List			
ListCompatibleImages	This action returns 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	Returns an array of JobListEntry objects of the specified length.	List			
ListLongTermPricing	Grants permission to list LongTermPricingListEntry objects for the account making the request	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateCluster	While a cluster's ClusterState value is in the AwaitingQuorum state, you can update some of the information associated with a cluster.	Write			
UpdateJob	While a job's JobState value is New, you can update some of the information associated with a job.	Write			
UpdateJobShipment	Updates the state when a the shipment states changes to a different state.	Write			
UpdateLongTermStorage	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 [Available keys for conditions](#).

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 \(p. 1776\)](#)
- [Resource types defined by Amazon SNS \(p. 1780\)](#)
- [Condition keys for Amazon SNS \(p. 1780\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1780)		
CheckIfPhoneNumberOptedOut	Grants permission to accept <code>alpha/phoneNumber</code> and indicate whether the phone holder has opted out of receiving SMS messages from your account	Read			
ConfirmSubscription	Grants permission to verify endpoint owner's intent to receive messages by validating the token sent to the endpoint by an earlier <code>Subscribe</code> action	Write	topic* (p. 1780)		
CreatePlatformApplication	Grants permission to create <code>platform</code> 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 <code>endpoint</code> for a device and mobile app on one of the supported push notification services, such as GCM and APNS	Write			
CreateSMSsandboxDestination	Grants permission to add a <code>destination</code> phone number and send a one-time password (OTP) to that phone number for an AWS account	Write			

Service Authorization Reference
Service Authorization Reference
Amazon SNS

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* (p. 1780)		iam:PassRole
			aws:RequestTag/ \${TagKey} (p. 1780)		
DeleteEndpoint	Grants permission to delete the endpoint for a device and mobile app from Amazon SNS	Write			
DeletePlatformApplication	Grants permission to delete the platform application object for one of the supported push notification services, such as APNS and GCM	Write			
DeleteSMSSandboxAccount	Grants permission to delete the AWS account's verified or pending phone number	Write			
DeleteTopic	Grants permission to delete a topic and all its subscriptions	Write	topic* (p. 1780)		
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 the properties of a subscription	Read			
GetTopicAttributes	Grants permission to return all of the properties of a topic	Read	topic* (p. 1780)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListEndpointsByPlatform	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			
ListPhoneNumberOptOuts	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			
ListSubscriptionsByTopic	Grants permission to return a list of the subscriptions to a specific topic	List	topic* (p. 1780)		
ListTagsForResource	Grants permission to list all tags added to the specified Amazon SNS topic	Read	topic (p. 1780)		
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* (p. 1780)		
RemovePermissions	Grants permission to remove a statement from a topic's access control policy	Permissions management	topic* (p. 1780)		

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			
SetTopicAttribute	Grants permission to allow a topic owner to set an attribute of the topic to a new value	Write	topic* (p. 1780)		iam:PassRole
Subscribe	Grants permission to prepare to subscribe an endpoint by sending the endpoint a confirmation message	Write	topic* (p. 1780)		
				sns:Endpoint (p. 1780)	sns:Protocol (p. 1780)
TagResource	Grants permission to add tags to the specified Amazon SNS topic	Tagging	topic (p. 1780)		
				aws:RequestTag/ \${TagKey} (p. 1780)	aws:TagKeys (p. 1780)
Unsubscribe	Grants permission to delete a subscription	Write			
UntagResource	Grants permission to remove tags from the specified Amazon SNS topic	Tagging	topic (p. 1780)		
				aws:RequestTag/ \${TagKey} (p. 1780)	aws:TagKeys (p. 1780)
VerifySMSSandboxDestinationPhone	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 \(p. 1776\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
topic	<code>arn:\${Partition}:sns:\${Region}:\${Account}: \${TopicName}</code>	aws:ResourceTag/\${TagKey} (p. 1780)

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 [Available global condition keys](#).

Condition keys	Description	Type
aws:RequestTag/\${TagKey}	Filters access by tags from request	String
aws:ResourceTag/\${TagKey}	Filters access by tags associated with the resource	String
aws:TagKeys	Filters access by tag keys from request	ArrayOfString
sns:Endpoint	Filters access by the URL, email address, or ARN from a Subscribe request or a previously confirmed subscription	String
sns:Protocol	Filters access by the protocol value from a Subscribe request or a previously confirmed subscription	String

Actions, resources, and condition keys for 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 \(p. 1781\)](#)

- [Resource types defined by AWS SQL Workbench \(p. 1785\)](#)
- [Condition keys for AWS SQL Workbench \(p. 1785\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateConnection [permission only]	Grants permission to associate <code>connection</code> to a chart	Write	chart* (p. 1785)		
			connection* (p. 1785)		
AssociateConnection [permission only]	Grants permission to associate <code>connection</code> to a tab	Write	connection* (p. 1785)		
AssociateQueryWithTab [permission only]	Grants permission to associate <code>query</code> to a tab	Write	query* (p. 1785)		
BatchDeleteFolders [permission only]	Grants permission to delete folders on your account	Write			
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* (p. 1785)		
				aws:TagKeys (p. 1786)	
				aws:RequestTag/\${TagKey} (p. 1785)	
CreateConnection	Grants permission to create a new connection on your account	Write	connection* (p. 1785)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
[permission only]				aws:TagKeys (p. 1786) aws:RequestTag/\${TagKey} (p. 1785)	
CreateFolder [permission only]	Grants permission to create folder on your account	Write			
CreateSavedQuery [permission only]	Grants permission to create a new saved query on your account	Write	query* (p. 1785)		
				aws:TagKeys (p. 1786) aws:RequestTag/\${TagKey} (p. 1785)	
DeleteChart [permission only]	Grants permission to remove charts on your account	Write	chart* (p. 1785)		
DeleteConnection [permission only]	Grants permission to remove connections on your account	Write	connection* (p. 1785)		
DeleteSavedQuery [permission only]	Grants permission to remove saved queries on your account	Write	query* (p. 1785)		
DeleteTab [permission only]	Grants permission to remove a tab on your account	Write			
DriverExecute [permission only]	Grants permission to execute a query in your redshift cluster	Write	connection* (p. 1785)		
GenerateSession [permission only]	Grants permission to generate a new session on your account	Write			
GetAccountInfo [permission only]	Grants permission to get account info	Read			
GetChart [permission only]	Grants permission to get charts on your account	Read	chart* (p. 1785)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetConnection [permission only]	Grants permission to get connections on your account	Read	connection* (p. 1785)		
GetSavedQuery [permission only]	Grants permission to get saved query on your account	Read	query* (p. 1785)		
GetUserInfo [permission only]	Grants permission to get user info	Read			
GetUserWorkspaceSettings [permission only]	Grants permission to get workspace settings on your account	Read			
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			
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* (p. 1785)		
ListTabs [permission only]	Grants permission to list tabs on your account	List			
ListTaggedResources [permission only]	Grants permission to list tagged resources	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource [permission only]	Grants permission to list the tags of an sqlworkbench resource	Read	chart (p. 1785)		
			connection (p. 1785)		
			query (p. 1785)		
PutTab [permission only]	Grants permission to create or update a tab on your account	Write			
PutUserWorkspace [permission only]	Grants permission to update workspace settings on your account	Write			
TagResource [permission only]	Grants permission to tag an sqlworkbench resource	Tagging	chart (p. 1785)		
			connection (p. 1785)		
			query (p. 1785)		
			aws:TagKeys (p. 1786)		
			aws:RequestTag/ \${TagKey} (p. 1785)		
UntagResource [permission only]	Grants permission to untag an sqlworkbench resource	Tagging	chart (p. 1785)		
			connection (p. 1785)		
			query (p. 1785)		
			aws:TagKeys (p. 1786)		
			aws:RequestTag/ \${TagKey} (p. 1785)		
UpdateAccountExportSettings [permission only]	Grants permission to update account-wide export settings	Write			
UpdateChart [permission only]	Grants permission to update a chart on your account	Write	chart* (p. 1785)		
			aws:TagKeys (p. 1786)		
			aws:RequestTag/ \${TagKey} (p. 1785)		
UpdateConnection [permission only]	Grants permission to update a connection on your account	Write	connection* (p. 1785)		
			aws:TagKeys (p. 1786)		
			aws:RequestTag/ \${TagKey} (p. 1785)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateFileFolder [permission only]	Grants permission to move files on your account	Write	chart (p. 1785)		
			query (p. 1785)		
UpdateFolder [permission only]	Grants permission to update a folder's name and details on your account	Write			
UpdateSavedQuery [permission only]	Grants permission to update a saved query on your account	Write	query* (p. 1785)		
				aws:TagKeys (p. 1786)	
				aws:RequestTag/ \${TagKey} (p. 1785)	

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 \(p. 1781\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
connection	<code>arn:\${Partition}:sqlworkbench:\${Region}: \${Account}:connection/\${ResourceId}</code>	aws:ResourceTag/ \${TagKey} (p. 1785)
query	<code>arn:\${Partition}:sqlworkbench:\${Region}: \${Account}:query/\${ResourceId}</code>	aws:ResourceTag/ \${TagKey} (p. 1785)
chart	<code>arn:\${Partition}:sqlworkbench:\${Region}: \${Account}:chart/\${ResourceId}</code>	aws:ResourceTag/ \${TagKey} (p. 1785)

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 [Available global condition 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

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 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 \(p. 1786\)](#)
- [Resource types defined by Amazon SQS \(p. 1788\)](#)
- [Condition keys for Amazon SQS \(p. 1788\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1788)		
ChangeMessageVisibility	Grants permission to change the <code>Visibility</code> timeout of a specified message in a queue to a new value	Write	queue* (p. 1788)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateQueue	Grants permission to create a new queue, or returns the URL of an existing one	Write	queue* (p. 1788)		
DeleteMessage	Grants permission to delete the specified message from the specified queue	Write	queue* (p. 1788)		
DeleteQueue	Grants permission to delete the queue specified by the queue URL, regardless of whether the queue is empty	Write	queue* (p. 1788)		
GetQueueAttributes	Grants permission to get attributes for the specified queue	Read	queue* (p. 1788)		
GetQueueUrl	Grants permission to return the URL of an existing queue	Read	queue* (p. 1788)		
ListDeadLetterSourcequeues	Grants permission to return a list of your queues that have the RedrivePolicy queue attribute configured with a dead letter queue	Read	queue* (p. 1788)		
ListQueueTags	Grants permission to list tags added to an SQS queue	Read	queue* (p. 1788)		
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* (p. 1788)		
ReceiveMessage	Grants permission to retrieve one or more messages, with a maximum limit of 10 messages, from the specified queue	Read	queue* (p. 1788)		
RemovePermissions	Grants permission to revoke any permissions in the queue policy that matches the specified Label parameter	Permissions management	queue* (p. 1788)		
SendMessage	Grants permission to deliver a message to the specified queue	Write	queue* (p. 1788)		
SetQueueAttributes	Grants permission to set the value of one or more queue attributes	Write	queue* (p. 1788)		
TagQueue	Grants permission to add tags to the specified SQS queue	Tagging	queue* (p. 1788)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagQueue	Grants permission to remove tags from the specified SQS queue	Tagging	queue* (p. 1788)		

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 \(p. 1786\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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	<code>arn:\${Partition}:sqs:\${Region}:\${Account}: \${QueueName}</code>	

Condition keys for Amazon SQS

SQS 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 [Available keys for conditions](#).

Actions, resources, and condition keys for AWS SSO

AWS SSO (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 SSO \(p. 1788\)](#)
- [Resource types defined by AWS SSO \(p. 1795\)](#)
- [Condition keys for AWS SSO \(p. 1796\)](#)

Actions defined by AWS SSO

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually

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

The **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateDirectory	Grants permission to connect a directory to be used by AWS Single Sign-On	Write			ds:AuthorizeApplication
AssociateProfile	Grants permission to create an association between a directory user or group and a profile	Write			
AttachManagedPolicy	Grants permission to attach an AWS Managed Policy to a permission set	Permissions management	Instance* (p. 1796) PermissionSet* (p. 1795)		
CreateAccountAssignment	Grants permission to assign access to a Principal for a specified AWS account using a specified permission set	Write	Account* (p. 1795) Instance* (p. 1796) PermissionSet* (p. 1795)		
CreateApplication	Grants permission to add an application instance to AWS Single Sign-On	Write			
CreateApplicationCertificate	Grants permission to add a new certificate for an application instance	Write			
CreateInstanceAccess	Grants permission to enable the instance for AWS Guard and specify the attributes	Write	Instance* (p. 1796)		
CreateManagedApplication	Grants permission to add a managed application instance to AWS Single Sign-On	Write			
CreatePermissionSet	Grants permission to create a permission set	Write	Instance* (p. 1796)		
				aws:RequestTag/\${TagKey} (p. 1796)	
				aws:TagKeys (p. 1796)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateProfile	Grants permission to create a profile for an application instance	Write			
CreateTrust	Grants permission to create a federation trust in a target account	Write			
DeleteAccountAssignment	Grants permission to delete a principal's access from a specified AWS account using a specified permission set	Write	Account* (p. 1795)		
DeleteApplicationInstance	Grants permission to delete the application instance		Instance* (p. 1796)		
DeleteApplicationManagedCertificate	Grants permission to delete an inactive certificate from the application instance		PermissionSet* (p. 1795)		
DeleteInlinePolicy	Grants permission to delete the inline policy from a specified permission set	Write	Instance* (p. 1796)		
DeleteInstanceAccessControlList	Grants permission to disable ABAC controls over the configuration list for the instance		PermissionSet* (p. 1795)		
DeleteManagedApplication	Grants permission to delete the managed application instance	Write	Instance* (p. 1796)		
DeletePermissionSet	Grants permission to delete a permission set	Write	Instance* (p. 1796)		
DeletePermissionPolicy	Grants permission to delete the permission policy associated with a permission set		PermissionSet* (p. 1795)		
DeleteProfile	Grants permission to delete the profile for an application instance	Permissions management			
DescribeAccountAssignmentCreationRequest	Grants permission to describe the status of the assignment creation request	Read	Instance* (p. 1796)		
DescribeAccountAssignmentDeletionRequest	Grants permission to describe the status of an assignment deletion request	Read	Instance* (p. 1796)		
DescribeInstanceConfiguration	Grants permission to get the list of attributes used by the configuration instance for ABAC	Read	Instance* (p. 1796)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribePermissionSet	Grants permission to describe a permission set	Read	Instance* (p. 1796)		
	PermissionSet* (p. 1795)				
DescribePermissionSetStatusForTheGivenPermissionSetProvisioningRequest	Grants permission to describe the status for the given Permission Set Provisioning request	Read	Instance* (p. 1796)		
DescribePermissionsPoliciesAssociatedWithAPermissionSet	Grants permission to retrieve all the permissions policies associated with a permission set	Read			
DescribeRegisteredRegions	Grants permission to obtain the regions where your organization has enabled AWS Single Sign-on	Read			
DetachManagedPolicyFromAPermissionSet	Grants permission to detach the attached AWS managed policy from the specified permission set	Permissions management	Instance* (p. 1796)		
			PermissionSet* (p. 1795)		
DisassociateDirectoryFromAWSSSO	Grants permission to disassociate a directory to be used by AWS Single Sign-On	Write			ds:UnauthorizeApplication
DisassociateProfileFromAUserOrGroup	Grants permission to disassociate a directory user or group from a profile	Write			
GetApplicationInstanceDetails	Grants permission to retrieve details for an application instance	Read			
GetApplicationTemplateDetails	Grants permission to retrieve application template details	Read			
GetInlinePolicyForAPermissionSet	Grants permission to obtain the inline policy set assigned to the permission set	Read	Instance* (p. 1796)		
			PermissionSet* (p. 1795)		
GetManagedApplicationDetailsForAnApplication	Grants permission to retrieve details for an application instance	Read			
GetMfaDeviceManagementSettingsForADirectory	Grants permission to retrieve MFA Device Management settings for the directory	Read			
GetPermissionSetDetails	Grants permission to retrieve details of a permission set	Read			
GetPermissionsPoliciesAssociatedWithAPermissionSet	Grants permission to retrieve all permission policies associated with a permission set	Read			sso:DescribePermissionsPolicies

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetProfile	Grants permission to retrieve a profile for an application instance	Read			
GetSSOStatus	Grants permission to check if AWS Single Sign-On is enabled	Read			
GetSharedSsoConfiguration	Grants permission to retrieve configuration for the current SSO instance	Read			
GetSsoConfiguration	Grants permission to retrieve configuration for the current SSO instance	Read			
GetTrust	Grants permission to retrieve the federation trust in a target account	Read			
ImportApplication	Grants permission to update the application instance by metadata uploading an application SAML metadata file provided by the service provider	Write			
ListAccountAssignments	Grants permission to list the status of the AWS account assignment creation requests for a specified SSO instance	List	Instance* (p. 1796)		
ListAccountAssignmentDeletions	Grants permission to list the status of the AWS account assignment deletion requests for a specified SSO instance	List	Instance* (p. 1796)		
ListAccountAssignmentsForPermissionSet	Grants permission to list the assignments of the specified AWS account with the specified permission set	List	Account* (p. 1795)		
			Instance* (p. 1796)		
			PermissionSet* (p. 1795)		
ListAccountsForPermissionSet	Grants permission to list all the AWS accounts where the specified permission set is provisioned	List	Instance* (p. 1796)		
			PermissionSet* (p. 1795)		
ListApplicationInstances	Grants permission to retrieve all of the certificates for a given application instance	Read			
ListApplicationInstances	Grants permission to retrieve all application instances	List			sso:GetApplicationInstances
ListApplicationTemplates	Grants permission to retrieve all supported application templates	List			sso:GetApplicationTemplates

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListApplications	Grants permission to retrieve all supported applications	List			
ListDirectoryAssociations	Grants permission to retrieve details about the directory connected to AWS Single Sign-On	Read			
ListInstances	Grants permission to list the SSO Instances that the caller has access to	List			
ListManagedPolicies	Grants permission to list the AWS Managed Policies that are attached to a specified permission set	List	Instance* (p. 1796)		
ListPermissionSets	Grants permission to list the Status of the Permission Set Provisioning requests for a specified SSO instance		PermissionSet* (p. 1795)		
ListPermissionSet	Grants permission to retrieve all permission sets	List	Instance* (p. 1796)		
ListPermissionSets	Grants permission to list all the permission sets that are provisioned to a specified AWS account	List	Account* (p. 1795)		
ListProfileAssociations	Grants permission to retrieve the directory user or group associated with the profile		Instance* (p. 1796)		
ListProfiles	Grants permission to retrieve all profiles for an application instance	List	sso:GetProfile		
ListTagsForResource	Grants permission to list the tags that are attached to a specified resource	Read	Instance* (p. 1796)		
ProvisionPermissions	Grants permission to provision a specified permission set to the specified target		PermissionSet* (p. 1795)		
PutInlinePolicyToTarget	Grants permission to attach an IAM inline policy to a permission set	Write	Instance* (p. 1796)		
PutMfaDeviceManagement	Grants permission to put Mfa Device Management settings for the directory		PermissionSet* (p. 1795)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutPermissionsPolicy	Grants permission to add a policy to a permission set	Permissions management			
SearchGroups	Grants permission to search for groups within the associated directory	Read			ds:DescribeDirectories
SearchUsers	Grants permission to search for users within the associated directory	Read			ds:DescribeDirectories
StartSSO	Grants permission to initialize AWS Single Sign-On	Write			organizations:DescribeOrganizations organizations:EnableAWS
TagResource	Grants permission to associate a set of tags with a specified resource	Tagging	Instance* (p. 1796)		
			PermissionSet* (p. 1795)		
				aws:RequestTag/\${TagKey} (p. 1796)	
UntagResource	Grants permission to disassociate a set of tags from a specified resource	Tagging	Instance* (p. 1796)		
			PermissionSet* (p. 1795)		
				aws:RequestTag/\${TagKey} (p. 1796)	aws:TagKeys (p. 1796)
UpdateApplicationCertificateAsTheDefault	Grants permission to set a certificate as the default one for this application instance	Write			
UpdateApplicationDisplayDataForApp	Grants permission to update display data for an application instance	Write			
UpdateApplicationFederationResponseConfiguration	Grants permission to update federation response configuration for the application instance	Write			
UpdateApplicationFederationResponseSchemaConfiguration	Grants permission to update federation response schema configuration for the application instance	Write			
UpdateApplicationSecurityDetailsForTheConfiguration	Grants permission to update security details for the configuration application instance	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateApplicationServiceProviderRelatedConfiguration	Grants permission to update configuration for the application instance	Write			
UpdateApplicationStatusOfAnInstance	Grants permission to update the status of an application instance	Write			
UpdateDirectoryUserAttributeMappings	Grants permission to update the user attribute mappings for your connected directory	Write			
UpdateInstanceAttributeListWithConfiguration	Grants permission to update the attribute list with configuration instance for ABAC	Write	Instance* (p. 1796)		
UpdateManagedApplicationStatus	Grants permission to update the status of a managed application instance	Write			
UpdatePermissionSet	Grants permission to update the permission set	Permissions management	Instance* (p. 1796) PermissionSet* (p. 1795)		
UpdateProfile	Grants permission to update the profile for an application instance	Write			
UpdateSSOConfigurations	Grants permission to update the configuration for the current SSO instance	Write			
UpdateTrust	Grants permission to update the federation trust in a target account	Write			

Resource types defined by AWS SSO

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the [Actions table \(p. 1788\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1796)
Account	arn:\${Partition}:sso:::account/\${AccountId}	

Resource types	ARN	Condition keys
Instance	arn:\${Partition}:sso:::instance/\${InstanceId}	

Condition keys for AWS SSO

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

To view the global condition keys that are available to all services, see [Available global condition 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 SSO Directory

AWS SSO 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 SSO Directory \(p. 1796\)](#)
- [Resource types defined by AWS SSO Directory \(p. 1801\)](#)
- [Condition keys for AWS SSO Directory \(p. 1801\)](#)

Actions defined by AWS SSO 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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your

policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 SSO provides by default	Write			
CompleteVirtualMfaCreation	Grants permission to complete the creation process of a virtual MFA device	Write			
CompleteWebAuthnRegistration	Grants permission to complete the registration process of a WebAuthn device	Write			
CreateAlias	Grants permission to create an alias for the directory that AWS SSO provides by default	Write			
CreateBearerToken	Grants permission to create a bearer token for a given provisioning tenant	Write			
CreateExternalIdpProvider	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 SSO provides by default	Write			
CreateProvisioningTenant	Grants permission to create a provisioning tenant for a given directory	Write			
CreateUser	Grants permission to create a user in the directory that AWS SSO provides by default	Write			
DeleteBearerToken	Grants permission to delete a bearer token	Write			
DeleteExternalIdpProvider	Grants permission to delete the given external IdP certificate	Write			
DeleteExternalIdpProvider	Grants permission to delete an External Identity Provider configuration associated with the directory	Write			

Service Authorization Reference
Service Authorization Reference
AWS SSO Directory

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteGroup	Grants permission to delete a group from the directory that AWS SSO provides by default	Write			
DeleteMfaDevice	Grants permission to delete a MFA device by device name for a given user	Write			
DeleteProvisioning	Grants permission to delete the Provisioning tenant	Write			
DeleteUser	Grants permission to delete a user from the directory that AWS SSO provides by default	Write			
DescribeDirectory	Grants permission to retrieve information about the directory that AWS SSO provides by default	Read			
DescribeGroup	Grants permission to query the group data, not including user and group members	Read			
DescribeGroups	Grants permission to retrieve information about groups from the directory that AWS SSO provides by default	Read			
DescribeProvisioning	Grants permission to describe the Provisioning tenant	Read			
DescribeUser	Grants permission to retrieve information about a user from the directory that AWS SSO provides by default	Read			
DescribeUserByUserId	Grants permission to describe user with valid unique attribute represented for the user	Read			
DescribeUsers	Grants permission to retrieve information about user from the directory that AWS SSO provides by default	Read			
DisableExternalId	Grants permission to disable authentication of end users with an External Identity Provider	Write			
DisableUser	Grants permission to deactivate a user in the directory that AWS SSO provides by default	Write			

Service Authorization Reference
Service Authorization Reference
AWS SSO Directory

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableExternalIdPAuthenticationForEndUsers	Grants permission to enable authentication for end users with an External Identity Provider	Write			
EnableUser	Grants permission to activate user in the directory that AWS SSO provides by default	Write			
GetAWSSPConfig	Grants permission to retrieve the AWS SSO Service Provider configurations for the directory	Read			
 GetUserPoolInfo	(Deprecated) Grants permission to get UserPool Info	Read			
ImportExternalIdPcertificate	Grants permission to import the IdP certificate used for verifying external IdP responses	Write			
IsMemberInGroup	Grants permission to check if a member is a part of the group in the directory that AWS SSO provides by default	Read			
ListBearerTokens	Grants permission to list bearer tokens for a given provisioning tenant	Read			
ListExternalIdPCertificate	Grants permission to list the external IdP certificates of a given directory and IdP	Read			
ListExternalIdPConfigurations	Grants permission to list all the External Identity Provider configurations created for the directory	Read			
ListGroupsForMember	Grants permission to list groups of the target member	Read			
ListGroupsForUser	Grants permission to list groups for a user from the directory that AWS SSO provides by default	Read			
ListMembersInGroup	Grants permission to retrieve all members that are part of a group in the directory that AWS SSO provides by default	Read			
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			
RemoveMemberFromGroup	Grants permission to remove a member that is part of a group in the directory that AWS SSO provides by default	Write			
SearchGroups	Grants permission to search for groups within the associated directory	Read			
SearchUsers	Grants permission to search for users within the associated directory	Read			
StartVirtualMfaDevice	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			
UpdateExternalIdentities	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 SSO provides by default	Write			
UpdateGroupDisplayNames	Grants permission to update group display name update group display name response	Write			
UpdateMfaDevice	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 SSO provides by default	Write			
UpdateUser	Grants permission to update user information in the directory that AWS SSO provides by default	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateUserName	Grants permission to update user name update user name response	Write			
VerifyEmail	Grants permission to verify an email address of an User	Write			

Resource types defined by AWS SSO Directory

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

Condition keys for AWS SSO Directory

SSO Directory has no service-specific context keys that can be used in the Condition element of policy statements. For the list of the global context keys that are available to all services, see [Available keys for conditions](#).

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 \(p. 1801\)](#)
- [Resource types defined by AWS Step Functions \(p. 1804\)](#)
- [Condition keys for AWS Step Functions \(p. 1804\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1804)		
				aws:RequestTag/\${TagKey} (p. 1804)	
				aws:TagKeys (p. 1804)	
CreateStateMachine	Grants permission to create a state machine	Write	statemachine* (p. 1804)		
				aws:RequestTag/\${TagKey} (p. 1804)	
				aws:TagKeys (p. 1804)	
DeleteActivity	Grants permission to delete an activity	Write	activity* (p. 1804)		
DeleteStateMachine	Grants permission to delete a state machine	Write	statemachine* (p. 1804)		
DescribeActivity	Grants permission to describe an activity	Read	activity* (p. 1804)		
DescribeExecution	Grants permission to describe an execution	Read	execution* (p. 1804)		
DescribeStateMachine	Grants permission to describe a state machine	Read	statemachine* (p. 1804)		
DescribeStateMachineExecution	Grants permission to describe the State Machine for an execution	Read	execution* (p. 1804)		
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* (p. 1804)		
GetExecutionHistory	Grants permission to return the history of the specified execution as a list of events	Read	execution* (p. 1804)		
ListActivities	Grants permission to list the existing activities	List			
ListExecutions	Grants permission to list the executions of a state machine	Read	statemachine* (p. 1804)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListStateMachine	Grants permission to lists the existing state machines	List			
ListTagsForResource	Grants permission to list tags for an AWS Step Functions resource	Read	activity (p. 1804)		
			statemachine (p. 1804)		
SendTaskFailure	Grants permission to report that the task identified by the taskToken failed	Write			
SendTaskHeartbeat	Grants permission to report to the service that the task represented by the specified taskToken is still making progress	Write			
SendTaskSuccess	Grants permission to report that the task identified by the taskToken completed successfully	Write			
StartExecution	Grants permission to start a state machine execution	Write	statemachine* (p. 1804)		
StartSyncExecution	Grants permission to start a Synchronous Express state machine execution	Write	statemachine* (p. 1804)		
StopExecution	Grants permission to stop an execution	Write	execution* (p. 1804)		
TagResource	Grants permission to tag an AWS Step Functions resource	Tagging	activity (p. 1804)		
			statemachine (p. 1804)		
			aws:TagKeys (p. 1804)		
UntagResource	Grants permission to remove a tag from an AWS Step Functions resource	Tagging	activity (p. 1804)		
			statemachine (p. 1804)		
			aws:TagKeys (p. 1804)		
UpdateStateMachine	Grants permission to update a state machine	Write	statemachine* (p. 1804)		
			aws:RequestTag/ \${TagKey} (p. 1804)		
			aws:TagKeys (p. 1804)		

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 \(p. 1801\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
activity	<code>arn:\${Partition}:states:\${Region}: \${Account}:activity:\${ActivityName}</code>	aws:ResourceTag/\${TagKey} (p. 1804)
execution	<code>arn:\${Partition}:states:\${Region}: \${Account}:execution:\${StateMachineName}: \${ExecutionId}</code>	
statemachine	<code>arn:\${Partition}:states:\${Region}: \${Account}:stateMachine:\${StateMachineName}</code>	aws:ResourceTag/\${TagKey} (p. 1804)

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 [Available global condition 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	String

Actions, resources, and condition keys for Amazon Storage Gateway

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

References:

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

Topics

- [Actions defined by Amazon Storage Gateway \(p. 1805\)](#)
- [Resource types defined by Amazon Storage Gateway \(p. 1813\)](#)
- [Condition keys for Amazon Storage Gateway \(p. 1814\)](#)

Actions defined by Amazon Storage Gateway

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

The **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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} (p. 1814) aws:TagKeys (p. 1814)	
AddCache	Grants permission to configure one or more gateway local disks as cache for a cached-volume gateway	Write	gateway* (p. 1814)		
AddTagsToResource	Grants permission to add one or more tags to the specified resource	Tagging	gateway (p. 1814) share (p. 1814) tape (p. 1814) volume (p. 1814)	aws:RequestTag/\${TagKey} (p. 1814) aws:TagKeys (p. 1814)	
AddUploadBuffer	Grants permission to configure one or more gateway local disks as upload buffer for a specified gateway	Write	gateway* (p. 1814)		
AddWorkingStorage	Grants permission to configure one or more gateway local disks as working storage for a gateway	Write	gateway* (p. 1814)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssignTapePool	Grants permission to move a tape to the target pool specified	Write	tape* (p. 1814)		
	tapepool* (p. 1814)				
AssociateFileSystem	Grants permission to associate an Amazon FSx file system with the Amazon FSx file gateway	Write	gateway* (p. 1814)		
			aws:RequestTag/\${TagKey} (p. 1814)		
	aws:TagKeys (p. 1814)	AttachVolume	Grants permission to connect a volume to an iSCSI connection and then attaches the volume to the specified gateway	Write	gateway* (p. 1814)
	volume* (p. 1814)				
BypassGovernance	Grants permission to allow the governance retention lock on a pool to be bypassed	Write	tapepool* (p. 1814)		
CancelArchival	Grants permission to cancel archiving of a virtual tape to the virtual tape shelf (VTS) after the archiving process is initiated	Write	gateway* (p. 1814)		
	tape* (p. 1814)				
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* (p. 1814)		
	tape* (p. 1814)				
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* (p. 1814)		
	volume* (p. 1814)				
			aws:RequestTag/\${TagKey} (p. 1814)		
	aws:TagKeys (p. 1814)	CreateNFSFileShare	Grants permission to create a NFS file share on an existing file gateway	Write	gateway* (p. 1814)
	aws:RequestTag/\${TagKey} (p. 1814) aws:TagKeys (p. 1814)				
CreateSMBFileShare	Grants permission to create a SMB file share on an existing file gateway	Write	gateway* (p. 1814)		
			aws:RequestTag/\${TagKey} (p. 1814)	aws:TagKeys (p. 1814)	
CreateSnapshot	Grants permission to initiate a snapshot of a volume	Write	volume* (p. 1814)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSnapshotFromGateway	Grants permission to initiate a snapshot of a gateway from a volume recovery point	Write	volume* (p. 1814)		
CreateStorediSCSIVolume	Grants permission to create a volume on a specified gateway	Write	gateway* (p. 1814) aws:RequestTag/\${TagKey} (p. 1814) aws:TagKeys (p. 1814)		
CreateTapePool	Grants permission to create a tape pool	Write		aws:RequestTag/\${TagKey} (p. 1814) aws:TagKeys (p. 1814)	
CreateTapeWithBarcode	Grants permission to create a virtual tape by using your own barcode	Write	gateway* (p. 1814) tapepool* (p. 1814) aws:RequestTag/\${TagKey} (p. 1814) aws:TagKeys (p. 1814)		
CreateTapes	Grants permission to create one or more virtual tapes. You write data to the virtual tapes and then archive the tapes	Write	gateway* (p. 1814) tapepool* (p. 1814) aws:RequestTag/\${TagKey} (p. 1814) aws:TagKeys (p. 1814)		
DeleteAutomaticTapeDelivery	Grants permission to delete the automatic tape creation policy configured on a gateway-VTL	Write	gateway* (p. 1814)		
DeleteBandwidthLimits	Grants permission to delete the bandwidth rate limits of a gateway	Write	gateway* (p. 1814)		
DeleteChapCredentials	Grants permission to delete Challenge-Handshake Authentication Protocol (CHAP) credentials for a specified iSCSI target and initiator pair	Write	target* (p. 1814)		
DeleteFileShare	Grants permission to delete a file share from a file gateway	Write	share* (p. 1814)		
DeleteGateway	Grants permission to delete a gateway	Write	gateway* (p. 1814)		
DeleteSnapshot	Grants permission to delete a snapshot of a volume	Write	volume* (p. 1814)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTape	Grants permission to delete the specified virtual tape	Write	gateway* (p. 1814)		
			tape* (p. 1814)		
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* (p. 1814)		
DeleteVolume	Grants permission to delete the specified gateway volume that you previously created using the CreateCachediSCSIVolume or CreateStorediSCSIVolume API	Write	volume* (p. 1814)		
DescribeAvailability	Grants permission to get the information about the most recent high availability monitoring test that was performed on the gateway	Read	gateway* (p. 1814)		
DescribeBandwidth	Grants permission to get the rate limits of a gateway	Read	gateway* (p. 1814)		
DescribeBandwidthRateLimit	Grants permission to get the rate limit schedule of a gateway	Read	gateway* (p. 1814)		
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* (p. 1814)		
DescribeCachediSCSIVolumes	Grants permission to get descriptions of the gateway volumes specified in the request. This operation is supported only for the gateway-cached volume architecture	Read	volume* (p. 1814)		
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* (p. 1814)		
DescribeFileSystemAssociations	Grants permission to get a description for one or more file system associations	Read	fs-association* (p. 1814)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeGatewayMetadata	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* (p. 1814)		
DescribeMaintenanceTime	Grants permission to get your gateway's weekly maintenance start time including the day and time of the week	Read	gateway* (p. 1814)		
DescribeNFSFileShares	Grants permission to get a description for one or more file shares from a file gateway	Read	share* (p. 1814)		
DescribeSMBFileShares	Grants permission to get a description for one or more file shares from a file gateway	Read	share* (p. 1814)		
DescribeSMBSettings	Grants permission to get a description of a Server Message Block (SMB) file share settings from a file gateway	Read	gateway* (p. 1814)		
DescribeSnapshotSchedule	Grants permission to describe the snapshot schedule for the specified gateway volume	Read	volume* (p. 1814)		
DescribeStoredSCVolumes	Grants permission to get the description of the gateway volumes specified in the request	Read	volume* (p. 1814)		
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* (p. 1814)		
DescribeTapes	Grants permission to get a description of the specified Amazon Resource Name (ARN) of virtual tapes	Read	gateway* (p. 1814)		
DescribeUploadBuffer	Grants permission to get information about the upload buffer of a gateway	Read	gateway* (p. 1814)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeVTLDevices	Grants permission to get a description of virtual tape library (VTL) devices for the specified gateway	Read	gateway* (p. 1814)		
DescribeWorkingStorage	Grants permission to get information about the working storage of a gateway	Read	gateway* (p. 1814)		
DetachVolume	Grants permission to disconnect a volume from an iSCSI connection and then detaches the volume from the specified gateway	Write	volume* (p. 1814)		
DisableGateway	Grants permission to disable a gateway when the gateway is no longer functioning	Write	gateway* (p. 1814)		
DisassociateFileSystems	Grants permission to disassociate an Amazon FSx file system from an Amazon FSx file gateway	Write	fs-association* (p. 1814)		
JoinDomain	Grants permission to enable you to join an Active Directory Domain	Write	gateway* (p. 1814)		
ListAutomaticTapeCreationPolicies	Grants permission to list the automatic tape creation policies configured on the specified gateway-VTL or all gateway-VTLs owned by your account	List	gateway* (p. 1814)		
ListFileShares	Grants permission to get a list of the file shares for a specific file gateway, or the list of file shares that belong to the calling user account	List	gateway* (p. 1814)		
ListFileSystemAssociations	Grants permission to get a list of the file system associations for the specified gateway	List	gateway* (p. 1814)		
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* (p. 1814)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to get the tags that have been added to the specified resource	List	gateway (p. 1814)		
	share (p. 1814)				
	tape (p. 1814)				
	volume (p. 1814)				
ListTapePools	Grants permission to list tape pools owned by your AWS account	List	tapepool* (p. 1814)		
ListTapes	Grants permission to list virtual tapes in your virtual tape library (VTL) and your virtual tape shelf (VTS)	List	tape* (p. 1814)		
ListVolumeInitiators	Grants permission to list iSCSI initiators that are connected to a volume	List	volume* (p. 1814)		
ListVolumeRecoveryPoints	Grants permission to list the recovery points for a specified gateway	List	gateway* (p. 1814)		
ListVolumes	Grants permission to list the iSCSI stored volumes of a gateway	List	gateway* (p. 1814)		
NotifyWhenUploads	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* (p. 1814)		
RefreshCache	Grants permission to refresh the cache for the specified file share	Write	share* (p. 1814)		
RemoveTagsFromResource	Grants permission to remove one or more tags from the specified resource	Tagging	gateway (p. 1814)		
	share (p. 1814)				
	tape (p. 1814)				
	volume (p. 1814)				
	aws:TagKeys (p. 1814)				
ResetCache	Grants permission to reset all cache disks that have encountered an error and makes the disks available for reconfiguration as cache storage	Write	gateway* (p. 1814)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RetrieveTapeArchive	Grants permission to retrieve an archived virtual tape from the virtual tape shelf (VTS) to a gateway-VTL	Write	gateway* (p. 1814)		
			tape* (p. 1814)		
RetrieveTapeRecoveryPoint	Grants permission to retrieve the recovery point for the specified virtual tape	Write	gateway* (p. 1814)		
			tape* (p. 1814)		
SetLocalConsolePassword	Grants permission to set the password for your VM local console	Write	gateway* (p. 1814)		
SetSMBGuestPassword	Grants permission to set the password for SMB Guest user	Write	gateway* (p. 1814)		
ShutdownGateway	Grants permission to shut down a gateway	Write	gateway* (p. 1814)		
StartAvailabilityMonitoring	Grants permission to start a test that verifies that the specified gateway is configured for High Availability monitoring in your host environment	Write	gateway* (p. 1814)		
StartGateway	Grants permission to start a gateway that you previously shut down	Write	gateway* (p. 1814)		
UpdateAutomaticTapeRotation	Grants permission to update the automatic tape rotation policy configured on a gateway-VTL	Write	gateway* (p. 1814)		
			tapestream* (p. 1814)		
UpdateBandwidthLimit	Grants permission to update the bandwidth rate limits of a gateway	Write	gateway* (p. 1814)		
UpdateBandwidthSchedule	Grants permission to update the bandwidth schedule of a gateway	Write	gateway* (p. 1814)		
UpdateChapCredentials	Grants permission to update the Challenge-Handshake Authentication Protocol (CHAP) credentials for a specified iSCSI target	Write	target* (p. 1814)		
UpdateFileSystemAssociation	Grants permission to update a file system association	Write	fs-association* (p. 1814)		
UpdateGatewayInfo	Grants permission to update a gateway's metadata, which includes the gateway's name and time zone	Write	gateway* (p. 1814)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateGatewaySoftware	Grants permission to update the gateway's virtual machine (VM) software	Write	gateway* (p. 1814)		
UpdateMaintenanceTime	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* (p. 1814)		
UpdateNFSFileShares	Grants permission to update a NFS file share	Write	share* (p. 1814)		
UpdateSMBFileShares	Grants permission to update a SMB file share	Write	share* (p. 1814)		
UpdateSMBFileSharesVisibility	Grants permission to update whether the shares on a gateway are visible in a net view or browse list	Write	gateway* (p. 1814)		
UpdateSMBLocalUserGroups	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* (p. 1814)		
UpdateSMBSecurityStrategy	Grants permission to update the SMB security strategy on a file gateway	Write	gateway* (p. 1814)		
UpdateSnapshotSchedule	Grants permission to update a snapshot schedule configured for a gateway volume	Write	volume* (p. 1814)		
UpdateVTLDeviceType	Grants permission to update the type of medium changer in a gateway-VTL	Write	device* (p. 1814)		

Resource types defined by Amazon Storage Gateway

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the [Actions table](#) (p. 1805) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
device	arn:\${Partition}:storagegateway:\${Region}: \${Account}:gateway/\${GatewayId}/device/ \${Vtldevice}	
fs-association	arn:\${Partition}:storagegateway:\${Region}: \${Account}:fs-association/\${FsaId}	aws:ResourceTag/ \${TagKey} (p. 1814)
gateway	arn:\${Partition}:storagegateway:\${Region}: \${Account}:gateway/\${GatewayId}	aws:ResourceTag/ \${TagKey} (p. 1814)
share	arn:\${Partition}:storagegateway:\${Region}: \${Account}:share/\${ShareId}	aws:ResourceTag/ \${TagKey} (p. 1814)
tape	arn:\${Partition}:storagegateway:\${Region}: \${Account}:tape/\${TapeBarcode}	aws:ResourceTag/ \${TagKey} (p. 1814)
tapepool	arn:\${Partition}:storagegateway:\${Region}: \${Account}:tapepool/\${PoolId}	aws:ResourceTag/ \${TagKey} (p. 1814)
target	arn:\${Partition}:storagegateway:\${Region}: \${Account}:gateway/\${GatewayId}/target/ \${IscsiTarget}	
volume	arn:\${Partition}:storagegateway:\${Region}: \${Account}:gateway/\${GatewayId}/volume/ \${VolumeId}	aws:ResourceTag/ \${TagKey} (p. 1814)

Condition keys for Amazon Storage Gateway

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

To view the global condition keys that are available to all services, see [Available global condition 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 Sumerian

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

References:

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

Topics

- [Actions defined by Amazon Sumerian \(p. 1815\)](#)
- [Resource types defined by Amazon Sumerian \(p. 1815\)](#)
- [Condition keys for Amazon Sumerian \(p. 1816\)](#)

Actions defined by Amazon Sumerian

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

The **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Login [permission only]	Grants permission to log into the Sumerian console	Write			
ViewRelease [permission only]	Grants permission to view a project release	Read	project* (p. 1816)		

Resource types defined by Amazon Sumerian

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the [Actions table \(p. 1815\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
project	arn:\${Partition}:sumerian:\${Region}: \${Account}:project:\${ProjectName}	

Condition keys for Amazon Sumerian

Sumerian 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 [Available keys for conditions](#).

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 \(p. 1816\)](#)
- [Resource types defined by AWS Support \(p. 1818\)](#)
- [Condition keys for AWS Support \(p. 1818\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Note

AWS 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
AddAttachments	Adds one or more attachments <small>To an AWS Support case.</small>	Write			
AddCommunicationAttachments	Adds a customer communication <small>To an AWS Support case.</small>	Write			
CreateCase	Creates a new AWS Support case.	Write			
DescribeAttachment	Returns the description for an attachment.	Read			
DescribeCaseAttributes	This is an internally managed attribute which allows secondary services to read AWS Support case attributes.	Read			
DescribeCases	Returns a list of AWS Support cases that matches the given inputs.	Read			
DescribeCommunications	Returns the communications and attachments for one or more AWS Support cases.	Read			
DescribeIssueTypes	Returns issue types for AWS Support cases.	Read			
DescribeServices	Returns the current list of AWS services and categories that applies to each service.	Read			
DescribeSeverityLevels	Returns the list of severity levels <small>that can be assigned to an AWS Support case.</small>	Read			
DescribeSupportLevel	Returns the support level for an AWS Account identifier.	Read			
DescribeTrustedAdvisorRefreshedCheck	Returns the status of a Trusted Advisor refresh check based on a list of check identifiers.	Read			
DescribeTrustedAdvisorSearch	Returns the results of the Trusted Advisor check that has the specified check identifier.	Read			
DescribeTrustedAdvisorSummaries	Returns the summaries of the results of the Trusted Advisor checks that have the specified check identifiers.	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeTrustedAdvisorChecks	Returns a list of all available Trusted Advisor checks, including name, identifier, category and description.	Read			
InitiateCallForCase	This is an internally managed function to initiate a call on AWS Support Center.	Write			
InitiateChatForCase	This is an internally managed function to initiate a chat on AWS Support Center.	Write			
PutCaseAttribute	This is an internally managed function which allows secondary services to attach attributes to AWS Support cases.	Write			
RateCaseCommunication	Rate an AWS Support case communication.	Write			
RefreshTrustedAdvisorCheck	Requests a refresh of the Trusted Advisor check that has the specified check identifier.	Write			
ResolveCase	Resolves an AWS Support case.	Write			
SearchForCases	Returns a list of AWS Support cases that matches the given inputs.	Read			

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 [Available keys for conditions](#).

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 \(p. 1819\)](#)
- [Resource types defined by AWS Sustainability \(p. 1819\)](#)
- [Condition keys for AWS Sustainability \(p. 1819\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCarbonFootprint	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 [Available keys for conditions](#).

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 \(p. 1820\)](#)
- [Resource types defined by AWS Systems Manager \(p. 1833\)](#)
- [Condition keys for AWS Systems Manager \(p. 1835\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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	automation-execution (p. 1834)		
			document (p. 1834)		
			maintenancewindow (p. 1834)		
			managed-instance (p. 1834)		
			opsitem (p. 1834)		
			opsmetadata (p. 1834)		
			parameter (p. 1834)		
			patchbaseline (p. 1835)		
AssociateOpsItem	Grants permission to associate RelatedItem to an OpsItem	Write	opsitem* (p. 1834)		
CancelCommand	Grants permission to cancel a specified Run Command command	Write			
CancelMaintenanceWindow	Grants permission to cancel an In progress maintenance window execution	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateActivation	Grants permission to create an activation that is used to register on-premises servers and virtual machines (VMs) with Systems Manager	Write			
CreateAssociation	Grants permission to associate a specified Systems Manager document with specified instances or other targets	Write	document* (p. 1834)		
			instance (p. 1834)		
			managed-instance (p. 1834)		
CreateAssociationBatch	Grants permission to combine entries for multiple CreateAssociation operations in a single command	Write	document* (p. 1834)		
			instance (p. 1834)		
			managed-instance (p. 1834)		
CreateDocument	Grants permission to create a Systems Manager SSM document	Write	document* (p. 1834)		iam:PassRole
				aws:RequestTag/\${TagKey} (p. 1835)	
				aws:TagKeys (p. 1835)	
CreateMaintenanceWindow	Grants permission to create a maintenance window	Write		aws:RequestTag/\${TagKey} (p. 1835)	
				aws:TagKeys (p. 1835)	
CreateOpsItem	Grants permission to create an OpsItem in OpsCenter	Write		aws:RequestTag/\${TagKey} (p. 1835)	
					aws:TagKeys (p. 1835)
CreateOpsMetadata	Grants permission to create an OpsMetadata object for an AWS resource	Write		aws:RequestTag/\${TagKey} (p. 1835)	
				aws:TagKeys (p. 1835)	
CreatePatchBaseline	Grants permission to create a patch baseline	Write		aws:RequestTag/\${TagKey} (p. 1835)	
				aws:TagKeys (p. 1835)	
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* (p. 1835)		
				ssm:SyncType (p. 1836)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 (p. 1833)		
			document (p. 1834)		
			instance (p. 1834)		
			managed-instance (p. 1834)		
DeleteDocument	Grants permission to delete a specified SSM document and its instance associations	Write	document* (p. 1834)		
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* (p. 1834)		
DeleteOpsMetadata	Grants permission to delete an OpsMetadata object	Write	opsmetadata* (p. 1834)		
DeleteParameter	Grants permission to delete a specified SSM parameter	Write	parameter* (p. 1834)		
DeleteParameters	Grants permission to delete multiple specified SSM parameters	Write	parameter* (p. 1834)		
DeletePatchBaseline	Grants permission to delete a specified patch baseline	Write	patchbaseline* (p. 1835)		
DeleteResourceDataSync	Grants permission to delete a specified resource data sync	Write	resourcedatasync* (p. 1835)		
			ssm:SyncType (p. 1836)		
DeregisterManagedInstance	Grants permission to deregister a specified on-premises server or virtual machine (VM) from Systems Manager	Write	managed-instance* (p. 1834)		
DeregisterPatchBaselineFromDefault	Grants permission to deregister a specified patch baseline from being the default patch baseline for a specified patch group	Write	patchbaseline* (p. 1835)		
DeregisterTargetFromMaintenanceWindow	Grants permission to deregister a specified target from a maintenance window	Write	maintenancewindow* (p. 1834)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions	
DeregisterTaskFromMaintenanceWindow	Grants permission to deregister a specified task from a maintenance window	Write	maintenancewindow* (p. 1834)			
DescribeActivationDetails	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				
DescribeAssociationDetails	Grants permission to view details about the specified association for a specified instance or target	Read	association (p. 1833)			
				document (p. 1834)		
				instance (p. 1834)		
				managed-instance (p. 1834)		
DescribeAssociationInformationForExecution	Grants permission to view information about a specified association execution	Read				
DescribeAssociationAllExecutions	Grants permission to view all executions for a specified association	Read				
DescribeAutomationDetails	Grants permission to view details about all active and terminated Automation executions	Read				
DescribeAutomationInformationForWorkflow	Grants permission to view information about all active and terminated step executions in an Automation workflow	Read				
DescribeAvailablePatches	Grants permission to view all patches eligible to include in a patch baseline	Read				
DescribeDocumentDetails	Grants permission to view details about a specified SSM document	Read	document* (p. 1834)			
DescribeDocumentInformation	Grants permission to display information about SSM document parameters in the Systems Manager console (internal Systems Manager action)	Read	document* (p. 1834)			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDocumentPermissions	Grants permission to view the permissions for a specified SSM document	Read	document* (p. 1834)		
DescribeEffectivePatchAssociations	Grants permission to view current Associations for a specified instance	Read	instance (p. 1834)		
			managed-instance (p. 1834)		
DescribeEffectivePatchBaselineDetails	Grants permission to view details about patch baselines currently associated with the specified patch baseline (Windows only)	Read	patchbaseline* (p. 1835)		
DescribeInstanceAssociations	Grants permission to view the status of associations for a specified instance	Read	instance (p. 1834)		
			managed-instance (p. 1834)		
DescribeInstanceDetails	Grants permission to view details about a specified instance	Read			
DescribeInstancePatchDetails	Grants permission to view status details about patches on a specified instance	Read			
DescribeInstancePatchGroupDetails	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			
DescribeInstanceAmazonEC2ConsoleRenderDetails	Grants permission to user's Amazon EC2 console to render managed instances' nodes	Read			
DescribeInventoryDeletionDetails	Grants permission to view details about a specified inventory deletion	Read			
DescribeMaintenanceWindowTaskInvocations	Grants permission to view details of a specified task invocation execution for a maintenance window	List			
DescribeMaintenanceWindowTaskInvocations	Grants permission to view details about the tasks that ran during a specified maintenance window execution	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeMaintenanceWindowExecutionDetails	Grants permission to view the execution details of a specified maintenance window	List	maintenancewindow* (p. 1834)		
DescribeMaintenanceWindowUpcomingExecutions	Grants permission to view details about upcoming executions of a specified maintenance window	List			
DescribeMaintenanceWindowTargets	Grants permission to view a list of the targets associated with a specified maintenance window	List	maintenancewindow* (p. 1834)		
DescribeMaintenanceWindowTasks	Grants permission to view a list of the tasks associated with a specified maintenance window	List	maintenancewindow* (p. 1834)		
DescribeMaintenanceWindows	Grants permission to view information about all or specified maintenance windows	List			
DescribeMaintenanceWindowTargetsForInstance	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			
DescribePatchGroupAggregatedStatus	Grants permission to view aggregated status details for patches for a specified patch group	List			
DescribePatchGroupInformation	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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeSessions	Grants permission to view a list of recent Session Manager sessions that meet the specified search criteria	List			
DisassociateOpsItemRelatedItems	Grants permission to disassociate RelatedItem from an OpsItem	Write	opsitem* (p. 1834)		
GetAutomationExecutionDetails	Grants permission to view details of a specified Automation execution	Read			
GetCalendarState	Grants permission to view the calendar state for a change calendar or a list of change calendars	Read	document* (p. 1834)		
GetCommandInvocationDetails	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			
GetDefaultPatchBaseline	Grants permission to view the current default patch baseline for a specified operating system type	Read	patchbaseline* (p. 1835)		
GetDeployablePatchBaseline	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* (p. 1834)		
					ssm:DocumentCategories (p. 1835)
GetInventory	Grants permission to view instance inventory details per the specified criteria	Read			
GetInventorySchemas	Grants permission to view a list of inventory types or attribute names for a specified inventory item type	Read			
GetMaintenanceWindowDetails	Grants permission to view details about a specified maintenance window	Read	maintenancewindow* (p. 1834)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetMaintenanceWindowDetailsAboutASpecifiedMaintenanceWindowExecution	Grants permission to view details about a specified maintenance window execution	Read			
GetMaintenanceWindowDetailsAboutATask	Grants permission to view details about a specified maintenance window execution task	Read			
GetMaintenanceWindowDetailsAboutATaskInvocation	Grants permission to view details about a task invocation maintenance window task running on a specific target	Read			
GetMaintenanceWindowDetailsAboutTasks	Grants permission to view details about tasks registered with a specified maintenance window	Read	maintenancewindow* (p. 1834)		
GetManifest[permissiononly]	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* (p. 1834)		
GetOpsMetadata	Grants permission to retrieve an OpsMetadata object	Read	opsmetadata* (p. 1834)		
GetOpsSummary	Grants permission to view summary information about OpsItems based on specified filters and aggregators	Read	resourcedatasync* (p. 1835)		
GetParameter	Grants permission to view information about a specified parameter	Read	parameter* (p. 1834)		
GetParameterHistory	Grants permission to view details and changes for a specified parameter	Read	parameter* (p. 1834)		
GetParameters	Grants permission to view information about multiple specified parameters	Read	parameter* (p. 1834)		
GetParametersByPath	Grants permission to view information about parameters in a specified hierarchy	Read	parameter* (p. 1834)		ssm:Recursive (p. 1835)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetPatchBaseline	Grants permission to view information about a specified patch baseline	Read	patchbaseline* (p. 1835)		
GetPatchBaselineForPatchGroup	Grants permission to view the ID of the current patch baseline for a specified patch group	Read	patchbaseline* (p. 1835)		
GetServiceSetting	Grants permission to view the account-level setting for an AWS service	Read	servicesetting* (p. 1835)		
LabelParameterVersion	Grants permission to apply an identifying label to a specified version of a parameter	Write	parameter* (p. 1834)		
ListAssociationVersions	Grants permission to list versions of the specified association	List			
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	Read			
ListCommands	Grants permission to list the commands sent to a specified instance	Read			
ListComplianceDetails	Grants permission to list compliance status for specified resource types on a specified resource	List			
ListComplianceSummary	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* (p. 1834)		
ListDocumentVersions	Grants permission to list all versions of a specified document	List	document* (p. 1834)		
ListDocuments	Grants permission to view information about a specified SSM document	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListInstanceAssociations	Grants permission to SSM Agent to check for new State Manager associations (internal Systems Manager call)	List	instance (p. 1834)		
			managed-instance (p. 1834)		
ListInventoryEntries	Grants permission to view a list of specified inventory types for a specified instance	List			
ListOpsItemEvents	Grants permission to view details about OpsItemEvents	Read			
ListOpsItemRelatedItems	Grants permission to view details about OpsItem RelatedItems	Read			
ListOpsMetadata	Grants permission to view a list of OpsMetadata objects	List			
ListResourceComplianceLevelSummary	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 (p. 1836)	
ListTagsForResource	Grants permission to view a list of resource tags for a specified resource	Read	automation-execution (p. 1834)		
	document (p. 1834)				
	maintenancewindow (p. 1834)				
	managed-instance (p. 1834)				
	opsitem (p. 1834)				
	opsmetadata (p. 1834)				
	parameter (p. 1834)				
	patchbaseline (p. 1835)				
ModifyDocument	Grants permission to share a custom SSM document publicly or privately with specified AWS accounts	Permissions management	document* (p. 1834)		
PutComplianceControl	Grants permission to register a compliance type and other compliance details on a specified resource	Write	instance (p. 1834)		
	managed-instance (p. 1834)				

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutConfigurePackagingResults [permission only]	Grants permission to SSM Agent to generate a report of the results of specific agent requests (internal Systems Manager call)	Read			
PutInventory	Grants permission to add or update inventory items on multiple specified managed instances	Write			
PutParameter	Grants permission to create an SSM parameter	Write	parameter* (p. 1834) aws:RequestTag/\${TagKey} (p. 1835) aws:TagKeys (p. 1835) ssm:Overwrite (p. 1835)		
RegisterDefaultPatchBaseline	Grants permission to specify the default patch baseline for an operating system type	Write	patchbaseline* (p. 1835)		
RegisterManagedSystemsManagerAgent	Grants permission to register a Systems Manager Agent	Write	aws:RequestTag/\${TagKey} (p. 1835) aws:TagKeys (p. 1835)		
RegisterPatchBaseline	Grants permission to specify the default patch baseline for a specified patch group	Write	patchbaseline* (p. 1835)		
RegisterTargetWithMaintenanceWindow	Grants permission to register a target with a specified maintenance window	Write	maintenancewindow* (p. 1834)		
RegisterTaskWithMaintenanceWindow	Grants permission to register a task with a specified maintenance window	Write	maintenancewindow* (p. 1834)		
RemoveTagsFromResource	Grants permission to remove a specified tag key from a specified resource	Tagging	automation-execution (p. 1834) document (p. 1834) maintenancewindow (p. 1834) managed-instance (p. 1834) opsitem (p. 1834) opsmetadata (p. 1834) parameter (p. 1834) patchbaseline (p. 1835)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ResetServiceSetting	Grants permission to reset the service setting for an AWS account to the default value	Write	servicesetting* (p. 1835)		
ResumeSession	Grants permission to reconnect a Session Manager session to a managed instance	Write	session* (p. 1835)		
SendAutomationSignal	Grants permission to send a Signal to change the current behavior or status of a specified Automation execution	Write			
SendCommand	Grants permission to run commands on one or more specified managed instances	Write	document* (p. 1834)		
			bucket (p. 1834)		
			instance (p. 1834)		
			managed-instance (p. 1834)		
				aws:ResourceTag/\${TagKey} (p. 1835) ssm:resourceTag/tag-key (p. 1836)	
StartAssociations	Grants permission to run a specified association manually	Write	association* (p. 1833)		
StartAutomationExecution	Grants permission to initiate the execution of an Automation document	Write	automation-definition* (p. 1834)		
StartChangeRequestExecution	Grants permission to initiate the execution of an Automation Change Template document	Write	automation-definition* (p. 1834)		
StartSession	Grants permission to initiate a connection to a specified target for a Session Manager session	Write	document (p. 1834)		
			instance (p. 1834)		
			managed-instance (p. 1834)		
				task (p. 1835)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ssm:SessionDocumentAccessCheck (p. 1834) ssm:resourceTag/tag-key (p. 1836) aws:ResourceTag/\${TagKey} (p. 1835)
StopAutomation	Grants permission to stop a Specified Automation execution that is already in progress	Write			
TerminateSession	Grants permission to permanently end a Session Manager connection to an instance	Write	session* (p. 1835)		
UnlabelParameter	Grants permission to remove an Identifying label from a specified version of a parameter	Write	parameter* (p. 1834)		
UpdateAssociation	Grants permission to update an association and immediately run the association on the specified targets	Write	association* (p. 1833)		
			document (p. 1834)		
			instance (p. 1834)		
			managed-instance (p. 1834)		
UpdateAssociationStatus	Grants permission to update the status of the SSM document associated with a specified instance	Write	document* (p. 1834)		
			instance (p. 1834)		
			managed-instance (p. 1834)		
UpdateDocument	Grants permission to update one or more values for an SSM document	Write	document* (p. 1834)		
UpdateDocumentDefaultVersion	Grants permission to change the defaultVersion of an SSM document	Write	document* (p. 1834)		
UpdateDocumentMetadata	Grants permission to update the Metadata of an SSM document	Write	document* (p. 1834)		
UpdateInstanceState [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* (p. 1833)		
			instance (p. 1834)		
			managed-instance (p. 1834)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateInstanceInfo	Grants permission to SSM Agent to send a heartbeat signal to the Systems Manager service in the cloud	Write			
UpdateMaintenanceWindow	Grants permission to update a specified maintenance window	Write	maintenancewindow* (p. 1834)		
UpdateMaintenanceWindowTarget	Grants permission to update a specified maintenance window target	Write	maintenancewindow* (p. 1834)		
UpdateMaintenanceWindowTask	Grants permission to update a specified maintenance window task	Write	maintenancewindow* (p. 1834)		
UpdateManagedInstanceIamRole	Grants permission to assign or change the IAM role assigned to a specified managed instance	Write	managed-instance* (p. 1834)		
UpdateOpsItem	Grants permission to edit or change an OpsItem	Write	opsitem* (p. 1834)		
UpdateOpsMetadata	Grants permission to update an OpsMetadata object	Write	opsmetadata* (p. 1834)		
UpdatePatchBaseline	Grants permission to update a specified patch baseline	Write	patchbaseline* (p. 1835)		
UpdateResourceDataSync	Grants permission to update a resource data sync	Write	resourcedatasync* (p. 1835)	ssm:SyncType (p. 1836)	
UpdateServiceSetting	Grants permission to update the service setting for an AWS account	Write	servicesetting* (p. 1835)		

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 \(p. 1820\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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}	

Resource types	ARN	Condition keys
automation-execution	arn:\${Partition}:ssm:\${Region}: \${Account}:automation-execution/ \${AutomationExecutionId}	aws:ResourceTag/ \${TagKey} (p. 1835) ssm:resourceTag/tag-key (p. 1836)
automation-definition	arn:\${Partition}:ssm:\${Region}: \${Account}:automation-definition/ \${AutomationDefinitionName}: \${VersionId}	
bucket	arn:\${Partition}:s3:::\${BucketName}	
document	arn:\${Partition}:ssm:\${Region}: \${Account}:document/\${DocumentName}	aws:ResourceTag/ \${TagKey} (p. 1835) ssm:resourceTag/tag-key (p. 1836)
instance	arn:\${Partition}:ec2:\${Region}: \${Account}:instance/\${InstanceId}	aws:ResourceTag/ \${TagKey} (p. 1835) ssm:resourceTag/tag-key (p. 1836)
maintenancewindow	arn:\${Partition}:ssm:\${Region}: \${Account}:maintenancewindow/\${ResourceId}	aws:ResourceTag/ \${TagKey} (p. 1835) ssm:resourceTag/tag-key (p. 1836)
managed-instance	arn:\${Partition}:ssm:\${Region}: \${Account}:managed-instance/\${InstanceId}	aws:ResourceTag/ \${TagKey} (p. 1835) ssm:resourceTag/tag-key (p. 1836)
managed-instance-inventory	arn:\${Partition}:ssm:\${Region}: \${Account}:managed-instance-inventory/ \${InstanceId}	
opsitem	arn:\${Partition}:ssm:\${Region}: \${Account}:opsitem/\${ResourceId}	aws:ResourceTag/ \${TagKey} (p. 1835)
opsmetadata	arn:\${Partition}:ssm:\${Region}: \${Account}:opsmetadata/\${ResourceId}	aws:ResourceTag/ \${TagKey} (p. 1835) ssm:resourceTag/tag-key (p. 1836)
parameter	arn:\${Partition}:ssm: \${Region}: \${Account}:parameter/ \${ParameterNameWithoutLeadingSlash}	aws:ResourceTag/ \${TagKey} (p. 1835) ssm:resourceTag/tag-key (p. 1836)

Resource types	ARN	Condition keys
patchbaseline	arn:\${Partition}:ssm:\${Region}: \${Account}:patchbaseline/ \${PatchBaselineIdResourceId}	aws:ResourceTag/ \${TagKey} (p. 1835) ssm:resourceTag/tag-key (p. 1836)
session	arn:\${Partition}:ssm:\${Region}: \${Account}:session/\${SessionId}	
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}	
windowtask	arn:\${Partition}:ssm:\${Region}: \${Account}:windowtask/\${WindowTaskId}	
task	arn:\${Partition}:ecs:\${Region}: \${Account}:task/\${TaskId}	aws:ResourceTag/ \${TagKey} (p. 1835)

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 [Available global condition 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
ssm:DocumentCategory	Filters access by verifying that a user has permission to access a document belonging to a specific category enum	ArrayOfString
ssm:Overwrite	Controls whether Systems Manager parameters can be overwritten	String
ssm:Recursive	Filters access to Systems Manager parameters created in a hierarchical structure	String
ssm:SessionDocumentAccess	Filters access by verifying that a user has permission to access either the default Session Manager configuration	Bool

Condition keys	Description	Type
	document or the custom configuration document specified in a request	
ssm:SyncType	Filters access by verifying that a user also has access to the ResourceDataSync SyncType specified in the request	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 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 \(p. 1836\)](#)
- [Resource types defined by AWS Systems Manager GUI Connect \(p. 1837\)](#)
- [Condition keys for AWS Systems Manager GUI Connect \(p. 1837\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelConnection	Grants permission to terminate a GUI Connect session	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
[permission only]					
GetConnection [permission only]	Grants permission to get the metadata for a GUI Connect session	Read			
StartConnection [permission only]	Grants permission to start a GUI Connect session	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 [Available keys for conditions](#).

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 \(p. 1837\)](#)
- [Resource types defined by AWS Systems Manager Incident Manager \(p. 1840\)](#)
- [Condition keys for AWS Systems Manager Incident Manager \(p. 1840\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the **Resource** element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateReplicationSet	Grants permission to create a replication set	Write			iam:CreateServiceLinkedRole
CreateResponsePlan	Grants permission to create a response plan	Write			iam:PassRole
CreateTimelineEvent	Grants permission to create a timeline event for an incident record	Write	incident-record* (p. 1840)		
			response-plan* (p. 1840)		
DeleteIncidentRecord	Grants permission to delete an incident record	Write	incident-record* (p. 1840)		
DeleteReplicationSet	Grants permission to delete a replication set	Write	replication-set* (p. 1840)		
DeleteResourcePolicy	Grants permission to delete a resource policy from a response plan	Permissions management	response-plan* (p. 1840)		
DeleteResponsePlan	Grants permission to delete a response plan	Write	response-plan* (p. 1840)		
DeleteTimelineEvent	Grants permission to delete a timeline event	Write	incident-record* (p. 1840)		
GetIncidentRecord	Grants permission to view the contents of an incident record	Read	incident-record* (p. 1840)		
			response-plan* (p. 1840)		
GetReplicationSet	Grants permission to view the replication set	Read	replication-set* (p. 1840)		
GetResourcePolicy	Grants permission to view resource policies of a response plan	Read	response-plan* (p. 1840)		

Service Authorization Reference
 Service Authorization Reference
 AWS Systems Manager Incident Manager

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetResponsePlan	Grants permission to view the contents of a specified response plan	Read	response-plan* (p. 1840)		
GetTimelineEvent	Grants permission to view a timeline event	Read	incident-record* (p. 1840)		
			response-plan* (p. 1840)		
ListIncidentRecords	Grants permission to list the contents of all incident records	List			
ListRelatedItems	Grants permission to list related items of an incident records	List	incident-record* (p. 1840)		
			response-plan* (p. 1840)		
ListReplicationSets	Grants permission to list all replication sets	List			
ListResponsePlans	Grants permission to list all response plans	List			
ListTagsForResource	Grants permission to view a list of resource tags for a specified resource	Read	response-plan* (p. 1840)		
ListTimelineEvents	Grants permission to list all timeline events for an incident record	List	incident-record* (p. 1840)		
			response-plan* (p. 1840)		
PutResourcePolicy	Grants permission to put a resource policy on a response plan	Permissions management	response-plan* (p. 1840)		
StartIncident	Grants permission to start a new incident using a response plan	Write	response-plan* (p. 1840)		
TagResource	Grants permission to add tags to a response plan	Tagging	response-plan* (p. 1840)		
UntagResource	Grants permission to remove tags from a response plan	Tagging	response-plan* (p. 1840)		
UpdateDeletionProtection	Grants permission to update replication set deletion protection	Write	replication-set* (p. 1840)		
UpdateIncidentRecord	Grants permission to update the contents of an incident record	Write	incident-record* (p. 1840)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			response-plan* (p. 1840)		
UpdateRelatedItem	Grants permission to update related items of an incident record	Write	incident-record* (p. 1840)		
			response-plan* (p. 1840)		
UpdateReplicationSet	Grants permission to update a replication set	Write	replication-set* (p. 1840)		
			response-plan* (p. 1840)		iam:PassRole
UpdateResponsePlan	Grants permission to update the contents of a response plan	Write	incident-record* (p. 1840)		
			response-plan* (p. 1840)		
UpdateTimelineEvent	Grants permission to update a timeline event	Write	response-plan* (p. 1840)		
			incident-record* (p. 1840)		

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 \(p. 1837\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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}	
incident-record	arn:\${Partition}:ssm-incidents::\${Account}:incident-record/\${ResponsePlan}/\${IncidentRecord}	
replication-set	arn:\${Partition}:ssm-incidents::\${Account}:replication-set/\${ReplicationSet}	

Condition keys for AWS Systems Manager Incident Manager

Incident Manager 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 [Available keys for conditions](#).

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 \(p. 1841\)](#)
- [Resource types defined by AWS Systems Manager Incident Manager Contacts \(p. 1843\)](#)
- [Condition keys for AWS Systems Manager Incident Manager Contacts \(p. 1844\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1843)		
ActivateContactChannel	Grants permission to activate a contact's contact channel	Write	contactchannel* (p. 1843)		
AssociateContact [permission only]	Grants permission to use a contact in an escalation plan	Permissions management	contact* (p. 1843)		

Service Authorization Reference
 Service Authorization Reference
 AWS Systems Manager Incident Manager Contacts

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateContact	Grants permission to create a contact	Write	contact* (p. 1843)		ssm-contacts:AssociateContact
CreateContactChannel	Grants permission to create a contact channel for a contact	Write	contact* (p. 1843)		
DeactivateContactChannel	Grants permission to deactivate a contact's contact channel	Write	contactchannel* (p. 1843)		
DeleteContact	Grants permission to delete a contact	Write	contact* (p. 1843)		
DeleteContactChannel	Grants permission to delete a contact's contact channel	Write	contactchannel* (p. 1843)		
DeleteContactPolicy	Grants permission to delete a contact's resource policy	Write	contact* (p. 1843)		
DescribeEngagement	Grants permission to describe an engagement	Read	engagement* (p. 1843)		
DescribePage	Grants permission to describe a page	Read	page* (p. 1843)		
GetContact	Grants permission to get a contact	Read	contact* (p. 1843)		
GetContactChannel	Grants permission to get a contact's contact channel	Read	contactchannel* (p. 1843)		
GetContactPolicy	Grants permission to get a contact's resource policy	Read	contact* (p. 1843)		
ListContactChannels	Grants permission to list all of a contact's contact channels	List	contact* (p. 1843)		
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* (p. 1843)		
ListPagesByContact	Grants permission to list all pages sent to a contact	List	contact* (p. 1843)		
ListPagesByEngagement	Grants permission to list all pages created in an engagement	List	engagement* (p. 1843)		
ListTagsForResource	Grants permission to view a list of resource tags for a specified resource	Read	contact* (p. 1843)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutContactPolicy	Grants permission to add a resource policy to a contact	Write	contact* (p. 1843)		
SendActivationCode	Grants permission to send the activation code of a contact's contact channel	Write	contactchannel* (p. 1843)		
StartEngagement	Grants permission to start an engagement	Write	contact* (p. 1843)		
StopEngagement	Grants permission to stop an engagement	Write	engagement* (p. 1843)		
TagResource	Grants permission to add tags to a response plan	Tagging	contact* (p. 1843)		
UntagResource	Grants permission to remove tags from a response plan	Tagging	contact* (p. 1843)		
UpdateContact	Grants permission to update a contact	Write	contact* (p. 1843)		ssm-contacts:AssociateContact
UpdateContactChannel	Grants permission to update a contact's contact channel	Write	contactchannel* (p. 1843)		
UpdateContactPolicy	Grants permission to update a contact's resource policy	Write	contact* (p. 1843)		

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 \(p. 1841\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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}	
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}	

Condition keys for AWS Systems Manager Incident Manager Contacts

Incident Manager Contacts 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 [Available keys for conditions](#).

Actions, resources, and condition keys for AWS Tag Editor

AWS 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 AWS Tag Editor \(p. 1844\)](#)
- [Resource types defined by AWS Tag Editor \(p. 1845\)](#)
- [Condition keys for AWS Tag Editor \(p. 1845\)](#)

Actions defined by AWS 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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListResourceType [permission only]	Grants permission to retrieve the resource types currently supported by Tag Editor	List			

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

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

Condition keys for AWS 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 [Available keys for conditions](#).

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 \(p. 1845\)](#)
- [Resource types defined by AWS Tax Settings \(p. 1846\)](#)
- [Condition keys for AWS Tax Settings \(p. 1846\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in

a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetExemptions	Grants permission to view tax exemptions data	Read			
UpdateExemption	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 [Available keys for conditions](#).

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 \(p. 1846\)](#)
- [Resource types defined by Amazon Textract \(p. 1848\)](#)
- [Condition keys for Amazon Textract \(p. 1848\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 identity documents provided as input	Read			s3:GetObject
DetectDocumentText	Grants permission to detect text in document images	Read			s3:GetObject
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			
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	Write			s3:GetObject

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	instances of invoices or receipts within an image or pdf provided as input				

Resource types defined by Amazon Textract

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

Condition keys for Amazon Textract

Textract 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 [Available keys for conditions](#).

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 \(p. 1848\)](#)
- [Resource types defined by Amazon Timestream \(p. 1851\)](#)
- [Condition keys for Amazon Timestream \(p. 1851\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources (“`*`”) in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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
CreateDatabase	Grants permission to create a database in your account	Write	database* (p. 1851) aws:RequestTag/\${TagKey} (p. 1851) aws:TagKeys (p. 1851)		timestream:DescribeEndpoints
CreateScheduledQuery	Grants permission to create a scheduled query in your account	Write		aws:RequestTag/PassRole \${TagKey} (p. 1851) timestream:DescribeEndpoints aws:TagKeys (p. 1851)	
 CreateTable	Grants permission to create a table in your account	Write	table* (p. 1851) aws:RequestTag/\${TagKey} (p. 1851) aws:TagKeys (p. 1851)		timestream:DescribeEndpoints
DeleteDatabase	Grants permission to delete a database in your account	Write	database* (p. 1851)		timestream:DescribeEndpoints
DeleteScheduledQuery	Grants permission to delete a scheduled query in your account	Write	scheduled-query* (p. 1851)		timestream:DescribeEndpoints
DeleteTable	Grants permission to delete a table in your account	Write	table* (p. 1851)		timestream:DescribeEndpoints
DescribeDatabase	Grants permission to describe a database in your account	Read	database* (p. 1851)		timestream:DescribeEndpoints
DescribeEndpoint	Grants permission to describe timestream endpoints	List			
DescribeScheduledQuery	Grants permission to describe a scheduled query in your account	Read	scheduled-query* (p. 1851)		timestream:DescribeEndpoints
DescribeTable	Grants permission to describe a table in your account	Read	table* (p. 1851)		timestream:DescribeEndpoints
ExecuteScheduledQuery	Grants permission to execute a scheduled query in your account	Write	scheduled-query* (p. 1851)		timestream:DescribeEndpoints
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* (p. 1851)		timestream:DescribeEndpoints
ListScheduledQueries	Grants permission to list scheduled queries in your account	List			timestream:DescribeEndpoints

Service Authorization Reference
Service Authorization Reference
Amazon Timestream

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTables	Grants permission to list tables in your account	List	database* (p. 1851)		timestream:DescribeEndpoint
ListTagsForResource	Grants permission to list tags of a resource in your account	Read	database* (p. 1851)		timestream:DescribeEndpoint
	scheduled-query* (p. 1851)				
	table* (p. 1851)				
PrepareQuery	Grants permission to issue 'prepare queries'	Read	table* (p. 1851)		timestream:DescribeEndpoint timestream:Select
Select	Grants permission to issue 'select from table' queries	Read	table* (p. 1851)		timestream:DescribeEndpoint
SelectValues	Grants permission to issue 'select 1' queries	Read			timestream:DescribeEndpoint
TagResource	Grants permission to add tags to a resource	Tagging	database* (p. 1851)		timestream:DescribeEndpoint
scheduled-query* (p. 1851)					
table* (p. 1851)					
	aws:RequestTag/\${TagKey} (p. 1851) aws:TagKeys (p. 1851)				
UntagResource	Grants permission to remove a tag from a resource	Tagging	database* (p. 1851)		timestream:DescribeEndpoint
scheduled-query* (p. 1851)					
table* (p. 1851)					
	aws:TagKeys (p. 1851)				
UpdateDatabase	Grants permission to update a database in your account	Write	database* (p. 1851)		timestream:DescribeEndpoint
UpdateScheduledQuery	Grants permission to update a scheduled query in your account	Write	scheduled-query* (p. 1851)		timestream:DescribeEndpoint
UpdateTable	Grants permission to update a table in your account	Write	table* (p. 1851)		timestream:DescribeEndpoint
WriteRecords	Grants permission to ingest data to a table in your account	Write	table* (p. 1851)		timestream:DescribeEndpoint

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 \(p. 1848\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
database	<code>arn:\${Partition}:timestream:\${Region}: \${Account}:database/\${DatabaseName}</code>	aws:ResourceTag/\${TagKey} (p. 1851)
table	<code>arn:\${Partition}:timestream:\${Region}: \${Account}:database/\${DatabaseName}/table/ \${TableName}</code>	aws:ResourceTag/\${TagKey} (p. 1851)
scheduled-query	<code>arn:\${Partition}:timestream: \${Region}: \${Account}:scheduled-query/ \${ScheduledQueryName}</code>	aws:ResourceTag/\${TagKey} (p. 1851)

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters access by the presence of tag key-value pairs in the request	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters access by tag key-value pairs attached to the resource	String
<code>aws:TagKeys</code>	Filters access by the presence of tag keys 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 \(p. 1852\)](#)
- [Resource types defined by AWS Tiros \(p. 1852\)](#)
- [Condition keys for AWS Tiros \(p. 1852\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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			
GetQueryAnswer [permission only]	Grants permission to get VPC reachability query answers	Read			
GetQueryExplanation [permission only]	Grants permission to get VPC reachability query explanations	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 [Available keys for conditions](#).

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 \(p. 1853\)](#)
- [Resource types defined by Amazon Transcribe \(p. 1858\)](#)
- [Condition keys for Amazon Transcribe \(p. 1858\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 a <code>CallAnalyticsCategory</code> . Amazon Transcribe applies the conditions specified by your analytics categories to your call analytics jobs	Write			
CreateLanguageModel	Grants permission to create a <code>LanguageModel</code> custom language model	Write		aws:RequestTag s3:GetObject \${TagKey} (p. 1858) s3>ListBucket aws:TagKeys (p. 1858)	
CreateMedicalVocabulary	Grants permission to create a <code>MedicalVocabulary</code> custom vocabulary that you can use to change the way	Write		aws:RequestTag s3:GetObject \${TagKey} (p. 1858)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Amazon Transcribe Medical handles transcription of an audio file			aws:TagKeys (p. 1858)	
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:RequestTagGetObject \${TagKey} (p. 1858) aws:TagKeys (p. 1858)	
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:RequestTagGetObject \${TagKey} (p. 1858) aws:TagKeys (p. 1858)	
DeleteCallAnalyticsCategory	Grants permission to delete a call analytics category using its name from Amazon Transcribe	Write			
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			
DeleteLanguageModel	Grants permission to delete a previously created custom language model	Write	languagemodel* (p. 1858)		
DeleteMedicalTranscriptionJob	Grants permission to delete a previously submitted medical transcription job	Write	medicaltranscriptionjob* (p. 1858)		
DeleteMedicalVocabulary	Grants permission to delete a medical vocabulary from Amazon Transcribe	Write	medicalvocabulary* (p. 1858)		
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* (p. 1858)		
DeleteVocabulary	Grants permission to delete a vocabulary from Amazon Transcribe	Write	vocabulary* (p. 1858)		
DeleteVocabularyFilter	Grants permission to delete a vocabulary filter from Amazon Transcribe	Write	vocabularyfilter* (p. 1858)		

Service Authorization Reference
Service Authorization Reference
Amazon Transcribe

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeLanguageModel	Grants permission to return information about a custom language model	Read	languageModel* (p. 1858)		
GetCallAnalyticsCategory	Grants permission to retrieve information about a call analytics category	Read			
GetCallAnalyticsJob	Grants permission to return information about a call analytics job	Read			
GetMedicalTranscriptionJob	Grants permission to return information about a medical transcription job	Read	medicaltranscriptionjob* (p. 1858)		
GetMedicalVocabulary	Grants permission to get information about a medical vocabulary	Read	medicalvocabulary* (p. 1858)		
GetTranscriptionJob	Grants permission to return information about a transcription job	Read	transcriptionjob* (p. 1858)		
GetVocabulary	Grants permission to get information about a vocabulary	Read	vocabulary* (p. 1858)		
GetVocabularyFilter	Grants permission to get information about a vocabulary filter	Read	vocabularyfilter* (p. 1858)		
ListCallAnalyticsCategories	Grants permission to list call analytics categories that have 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			
ListMedicalTranscriptionJobs	Grants permission to list medical transcription jobs with the specified status	List			
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			

Service Authorization Reference
Service Authorization Reference
Amazon Transcribe

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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	S3GetObject (p. 1857) transcribe:OutputLocation (p. 1859)
StartMedicalStreamProtocolJob	Grants permission to start a protocol job where audio is streamed to Transcribe Medical and the transcription results are streamed to your application	Write			
StartMedicalStreamWebSocketJob	Grants permission to start a WebSocket job where audio is streamed to Transcribe Medical and the transcription results are streamed to your application	Write			
StartMedicalTranscriptionJob	Grants permission to start an asynchronous job to transcribe medical speech to text	Write		transcribe:OutputEncryptionKMSKeyId	S3GetObject (p. 1857) transcribe:OutputLocation (p. 1859) transcribe:OutputKey (p. 1859) aws:RequestTag/ \${TagKey} (p. 1858) aws:TagKeys (p. 1858)
StartStreamTranscriptionJob	Grants permission to start a bidirectional HTTP2 stream to transcribe speech to text in real time	Write			
StartStreamTranscriptionWebsocketJob	Grants permission to start a websocket stream to transcribe speech to text in real time	Write			

Service Authorization Reference
Service Authorization Reference
Amazon Transcribe

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartTranscriptionJob	Grants permission to start an asynchronous job to transcribe speech to text	Write		transcribe:OutputName (p. 1858)	s3:GetObject
TagResource	Grants permission to tag a resource with given key value pairs	Tagging		aws:RequestTag/\${TagKey} (p. 1858)	aws:TagKeys (p. 1858)
UntagResource	Grants permission to untag a resource with given key	Tagging		aws:TagKeys (p. 1858)	
UpdateCallAnalyticsCategory	Grants permission to update the CallAnalytics category with new values. The UpdateCallAnalyticsCategory operation overwrites all of the existing information with the values that you provide in the request	Write			
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* (p. 1858)	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* (p. 1858)	s3:GetObject	
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* (p. 1858)	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 \(p. 1853\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1858)
vocabulary	arn:\${Partition}:transcribe:\${Region}: \${Account}:vocabulary/\${VocabularyName}	aws:ResourceTag/\${TagKey} (p. 1858)
vocabularyfilter	arn:\${Partition}:transcribe:\${Region}: \${Account}:vocabulary-filter/ \${VocabularyFilterName}	aws:ResourceTag/\${TagKey} (p. 1858)
languagemodel	arn:\${Partition}:transcribe:\${Region}: \${Account}:language-model/\${ModelName}	aws:ResourceTag/\${TagKey} (p. 1858)
medicaltranscriptionjob	arn:\${Partition}:transcribe:\${Region}: \${Account}:medical-transcription-job/ \${JobName}	aws:ResourceTag/\${TagKey} (p. 1858)
medicalvocabulary	arn:\${Partition}:transcribe:\${Region}: \${Account}:medical-vocabulary/ \${VocabularyName}	aws:ResourceTag/\${TagKey} (p. 1858)
callanalyticsjob	arn:\${Partition}:transcribe:\${Region}: \${Account}:analytics-job/\${JobName}	
callanalyticscategory	arn:\${Partition}:transcribe:\${Region}: \${Account}:analytics-category/ \${CategoryName}	

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 [Available global condition 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

Condition keys	Description	Type
<code>transcribe:OutputBucketName</code>	Filters access based on the output bucket name included in the request	String
<code>transcribe:OutputEncryptionKeyId</code>	Filters access based on the KMS key id included in the request	String
<code>transcribe:OutputKey</code>	Filters access based on the output key included in the request	String
<code>transcribe:OutputLocation</code>	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 \(p. 1859\)](#)
- [Resource types defined by AWS Transfer Family \(p. 1862\)](#)
- [Condition keys for AWS Transfer Family \(p. 1862\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1862)		iam:PassRole
CreateServer	Grants permission to create a server	Write		aws:TagKeys (p. 1862) aws:RequestTag/\${TagKey} (p. 1862)	
CreateUser	Grants permission to add a user associated with a server	Write	server* (p. 1862)		iam:PassRole
				aws:TagKeys (p. 1862)	
				aws:RequestTag/\${TagKey} (p. 1862)	
CreateWorkflow	Grants permission to create a workflow	Write		aws:TagKeys (p. 1862) aws:RequestTag/\${TagKey} (p. 1862)	
DeleteAccess	Grants permission to delete access	Write	server* (p. 1862)		
DeleteServer	Grants permission to delete a server	Write	server* (p. 1862)		
DeleteSshPublicKey	Grants permission to delete an SSH public key from a user	Write	user* (p. 1862)		
DeleteUser	Grants permission to delete a user associated with a server	Write	user* (p. 1862)		
DeleteWorkflow	Grants permission to delete a workflow	Write	workflow* (p. 1862)		
DescribeAccess	Grants permission to describe an access assigned to a server	Read	server* (p. 1862)		
DescribeExecution	Grants permission to describe an execution associated with a workflow	Read	workflow* (p. 1862)		
DescribeSecurityPolicy	Grants permission to describe a security policy	Read			
DescribeServer	Grants permission to describe a server	Read	server* (p. 1862)		
DescribeUser	Grants permission to describe a user associated with a server	Read	user* (p. 1862)		
DescribeWorkflow	Grants permission to describe a workflow	Read	workflow* (p. 1862)		
ImportSshPublicKey	Grants permission to add an SSH public key to a user	Write	user* (p. 1862)		

Service Authorization Reference
Service Authorization Reference
AWS Transfer Family

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAccesses	Grants permission to list accesses	Read	server* (p. 1862)		
ListExecutions	Grants permission to list executions associated with a workflow	Read	workflow* (p. 1862)		
ListSecurityPolicies	Grants permission to list security policies	List			
ListServers	Grants permission to list servers	List			
ListTagsForResource	Grants permission to list tags for a server, a user, or a workflow	Read	server (p. 1862) user (p. 1862) workflow (p. 1862)		
ListUsers	Grants permission to list users associated with a server	List	server* (p. 1862)		
ListWorkflows	Grants permission to list workflows	List			
SendWorkflowStepCallback	Grants permission to send a callback for asynchronous custom steps	Write	workflow* (p. 1862)		
StartServer	Grants permission to start a server	Write	server* (p. 1862)		
StopServer	Grants permission to stop a server	Write	server* (p. 1862)		
TagResource	Grants permission to tag a server or a user	Tagging	server (p. 1862) user (p. 1862) workflow (p. 1862) aws:TagKeys (p. 1862) aws:RequestTag/ \${TagKey} (p. 1862)		
TestIdentityProvider	Grants permission to test a server's custom identity provider	Read	user* (p. 1862)		
UntagResource	Grants permission to untag a server, a user, or a workflow	Tagging	server (p. 1862) user (p. 1862) workflow (p. 1862) aws:TagKeys (p. 1862)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAccess	Grants permission to update access	Write			iam:PassRole
UpdateServer	Grants permission to update the configuration of a server	Write	server* (p. 1862)		iam:PassRole
UpdateUser	Grants permission to update the configuration of a user	Write	user* (p. 1862)		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 \(p. 1859\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
user	<code>arn:\${Partition}:transfer:\${Region}: \${Account}:user/\${ServerId}/\${UserName}</code>	aws:ResourceTag/ \${TagKey} (p. 1862)
server	<code>arn:\${Partition}:transfer:\${Region}: \${Account}:server/\${ServerId}</code>	aws:ResourceTag/ \${TagKey} (p. 1862)
workflow	<code>arn:\${Partition}:transfer:\${Region}: \${Account}:workflow/\${WorkflowId}</code>	aws:ResourceTag/ \${TagKey} (p. 1862)

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 [Available global condition 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 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 \(p. 1863\)](#)
- [Resource types defined by Amazon Translate \(p. 1864\)](#)
- [Condition keys for Amazon Translate \(p. 1864\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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			
DeleteParallelData	Grants permission to delete a Parallel Data	Write			
DeleteTerminology	Grants permission to delete a terminology	Write			
DescribeTextTranslati	Grants permission to get the properties associated with an asynchronous batch translation job	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetParallelData	Grants permission to get a Parallel Data	Read			
GetTerminology	Grants permission to retrieve a terminology	Read			
ImportTerminology	Grants permission to create or update a terminology, depending on whether or not one already exists for the given terminology name	Write			
ListParallelData	Grants permission to list Parallel Data associated with your account	List			
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			
StopTextTranslationJob	Grants permission to stop an asynchronous batch translation job that is in progress	Write			
TranslateText	Grants permission to translate text from a source language to a target language	Read			
UpdateParallelData	Grants permission to update an existing Parallel Data	Write			

Resource types defined by Amazon Translate

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

Condition keys for Amazon Translate

Translate 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 [Available keys for conditions](#).

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 \(p. 1865\)](#)
- [Resource types defined by AWS Trusted Advisor \(p. 1868\)](#)
- [Condition keys for AWS Trusted Advisor \(p. 1868\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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
DescribeAccount [permission only]	Grants permission to view the AWS Support plan and various AWS Trusted Advisor preferences	Read			
DescribeAccountAWS [permission only]	Grants permission to view if the AWS account has enabled or disabled AWS Trusted Advisor	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeCheckItem	Grants permission to view details for the check items	Read	checks* (p. 1868)		
DescribeCheckRefreshStatus	Grants permission to view the refresh statuses for AWS Trusted Advisor checks	Read	checks* (p. 1868)		
DescribeCheckSummaries	Grants permission to view AWS Trusted Advisor check summaries	Read	checks* (p. 1868)		
DescribeChecks	Grants permission to view details for AWS Trusted Advisor checks	Read			
DescribeNotificationPreferences [permission only]	Grants permission to view the notification preferences for the AWS account	Read			
DescribeOrganization [permission only]	Grants permission to view if the AWS account meets the requirements to enable the organizational view feature	Read			
DescribeOrganizations [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			
DescribeServiceMetrics [permission only]	Grants permission to view information about organizational view reports, such as the AWS Regions, check categories, check names, and resource statuses	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DownloadRisk	Grants permission to download a file that contains details about the risk in AWS Trusted Advisor Priority	Read			
ExcludeCheckItem [permission only]	Grants permission to exclude recommendations for AWS Trusted Advisor checks	Write	checks* (p. 1868)		
GenerateReport [permission only]	Grants permission to create a report for AWS Trusted Advisor checks in your organization	Write			
IncludeCheckItem [permission only]	Grants permission to include recommendations for AWS Trusted Advisor checks	Write	checks* (p. 1868)		
ListAccountsForPath [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			
ListOrganizationRoots [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			
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* (p. 1868)		
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			
UpdateNotificationPreferences [permission only]	Grants permission to update notification preferences for AWS Trusted Advisor	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 \(p. 1865\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
checks	<code>arn:\${Partition}:trustedadvisor:\${Region}:\${Account}:checks/\${CategoryCode}/\${CheckId}</code>	

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 [Available keys for conditions](#).

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 \(p. 1868\)](#)
- [Resource types defined by AWS WAF \(p. 1874\)](#)
- [Condition keys for AWS WAF \(p. 1875\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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* (p. 1874)		
CreateGeoMatchSet	Grants permission to create a GeoMatchSet	Write	geomatchset* (p. 1875)		
CreateIPSet	Grants permission to create an IPSet	Write	ipset* (p. 1874)		
CreateRateBasedRule	Grants permission to create a RateBasedRule for limiting the volume of requests from a single IP address	Write	ratebasedrule* (p. 1874)		
				aws:RequestTag/\${TagKey} (p. 1875)	aws:TagKeys (p. 1875)
CreateRegexMatchSet	Grants permission to create a RegexMatchSet	Write	regexmatchset* (p. 1875)		
CreateRegexPatternSet	Grants permission to create a RegexPatternSet	Write	regexpatternset* (p. 1875)		
CreateRule	Grants permission to create a Rule for filtering web requests	Write	rule* (p. 1874)		
				aws:RequestTag/\${TagKey} (p. 1875)	aws:TagKeys (p. 1875)
CreateRuleGroup	Grants permission to create a RuleGroup, which is a collection of predefined rules that you can use in a WebACL	Write	rulegroup* (p. 1875)		
				aws:RequestTag/\${TagKey} (p. 1875)	aws:TagKeys (p. 1875)
CreateSizeConstraintSet	Grants permission to create a SizeConstraintSet	Write	sizeconstraintset* (p. 1875)		
CreateSqlInjectionMatchSet	Grants permission to create an SqlInjectionMatchSet	Write	sqlinjectionmatchset* (p. 1875)		
CreateWebACL	Grants permission to create a WebACL, which contains rules for filtering web requests	Permissions management	webacl* (p. 1875)		aws:RequestTag/\${TagKey} (p. 1875)

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	(p. 1875)
CreateWebACLMigrationCloudFormation	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*	(p. 1875)	s3:PutObject
CreateXssMatchSet	Grants permission to create an XSSMatchSet, which you use to detect requests that contain cross-site scripting attacks	Write	xssmatchset*	(p. 1875)	
DeleteByteMatchSet	Grants permission to delete a ByteMatchSet	Write	bytematchset*	(p. 1874)	
DeleteGeoMatchSet	Grants permission to delete a GeoMatchSet	Write	geomatchset*	(p. 1875)	
DeleteIPSet	Grants permission to delete an IPSet	Write	ipset*	(p. 1874)	
DeleteLoggingConfiguration	Grants permission to delete the Logging Configuration from a web ACL	Write	webacl*	(p. 1875)	
DeletePermission	Grants permission to delete a PAM policy from a rule group	Permissions management	rulegroup*	(p. 1875)	
DeleteRateBasedRule	Grants permission to delete a RateBasedRule	Write	ratebasedrule*	(p. 1874)	
DeleteRegexMatchSet	Grants permission to delete a RegexMatchSet	Write	regexmatchset*	(p. 1875)	
DeleteRegexPatternSet	Grants permission to delete a RegexPatternSet	Write	regexpatternset*	(p. 1875)	
DeleteRule	Grants permission to delete a Rule	Write	rule*	(p. 1874)	
DeleteRuleGroup	Grants permission to delete a RuleGroup	Write	rulegroup*	(p. 1875)	
DeleteSizeConstraintSet	Grants permission to delete a SizeConstraintSet	Write	sizeconstraintset*	(p. 1875)	
DeleteSqlInjectionMatchSet	Grants permission to delete an SqlInjectionMatchSet	Write	sqlinjectionmatchset*	(p. 1875)	
DeleteWebACL	Grants permission to delete a WebACL	Permissions management	webacl*	(p. 1875)	
DeleteXssMatchSet	Grants permission to delete an XSSMatchSet	Write	xssmatchset*	(p. 1875)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetByteMatchSet	Grants permission to retrieve a ByteMatchSet	Read	bytematchset* (p. 1874)		
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* (p. 1875)		
GetIPSet	Grants permission to retrieve an IPSet	Read	ipset* (p. 1874)		
GetLoggingConfiguration	Grants permission to retrieve a LoggingConfiguration for a web ACL	Read	webacl* (p. 1875)		
GetPermissionPolicy	Grants permission to retrieve an IAM policy for a rule group	Read	rulegroup* (p. 1875)		
GetRateBasedRule	Grants permission to retrieve a RateBasedRule	Read	ratebasedrule* (p. 1874)		
GetRateBasedRuleBlockedIPAddresses	Grants permission to retrieve the array of IP addresses that are currently being blocked by a RateBasedRule	Read	ratebasedrule* (p. 1874)		
GetRegexMatchSet	Grants permission to retrieve a RegexMatchSet	Read	regexmatchset* (p. 1875)		
GetRegexPatternSet	Grants permission to retrieve a RegexPatternSet	Read	regexpatternset* (p. 1875)		
GetRule	Grants permission to retrieve a Rule	Read	rule* (p. 1874)		
GetRuleGroup	Grants permission to retrieve a RuleGroup	Read	rulegroup* (p. 1875)		
GetSampledRequests	Grants permission to retrieve detailed information about a sample set of web requests	Read	rule (p. 1874) webacl (p. 1875)		
GetSizeConstraint	Grants permission to retrieve a SizeConstraint	Read	sizeconstraintset* (p. 1875)		
GetSqlInjectionMatchSet	Grants permission to retrieve an SqlInjectionMatchSet	Read	sqlinjectionmatchset* (p. 1875)		
GetWebACL	Grants permission to retrieve a WebACL	Read	webacl* (p. 1875)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetXssMatchSet	Grants permission to retrieve an <code>XssMatchSet</code>	Read	xssmatchset* (p. 1875)		
ListActivatedRules	Grants permission to retrieve an array of <code>ActivatedRule</code> objects	List			
ListByteMatchSets	Grants permission to retrieve an array of <code>ByteMatchSetSummary</code> objects	List			
ListGeoMatchSets	Grants permission to retrieve an array of <code>GeoMatchSetSummary</code> objects	List			
ListIPSets	Grants permission to retrieve an array of <code>IPSetSummary</code> objects	List			
ListLoggingConfigurations	Grants permission to retrieve an array of <code>LoggingConfiguration</code> objects	List			
ListRateBasedRules	Grants permission to retrieve an array of <code>RuleSummary</code> objects	List			
ListRegexMatchSets	Grants permission to retrieve an array of <code>RegexMatchSetSummary</code> objects	List			
ListRegexPatternSets	Grants permission to retrieve an array of <code>RegexPatternSetSummary</code> objects	List			
ListRuleGroups	Grants permission to retrieve an array of <code>RuleGroup</code> objects	List			
ListRules	Grants permission to retrieve an array of <code>RuleSummary</code> objects	List			
ListSizeConstraintSets	Grants permission to retrieve an array of <code>SizeConstraintSetSummary</code> objects	List			
ListSqlInjectionMatchSets	Grants permission to retrieve an array of <code>SqlInjectionMatchSet</code> objects	List			
ListSubscribedRuleGroups	Grants permission to retrieve an array of <code>RuleGroup</code> objects that you are subscribed to	List			
ListTagsForResource	Grants permission to retrieve the tags for a resource	Read	ratebasedrule (p. 1874) rule (p. 1874)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			rulegroup (p. 1875)		
			webacl (p. 1875)		
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 LoggingConfiguration with a specified web ACL	Write	webacl* (p. 1875)		iam:CreateServiceLinkedRole
PutPermissionPolicy	Grants permission to attach an IAM policy to a rule group, to share the rule group between accounts	Permissions management	rulegroup* (p. 1875)		
TagResource	Grants permission to add a Tag to a resource	Tagging	ratebasedrule (p. 1874)		
rule (p. 1874)					
rulegroup (p. 1875)					
webacl (p. 1875)					
	aws:RequestTag/ \${TagKey} (p. 1875)				
UntagResource	Grants permission to remove a Tag from a resource	Tagging	aws:TagKeys (p. 1875)		
ratebasedrule (p. 1874)					
rule (p. 1874)					
rulegroup (p. 1875)					
webacl (p. 1875)					
UpdateByteMatchTuple	Grants permission to insert or delete ByteMatchTuple objects in a ByteMatchSet	Write	bytematchset* (p. 1874)		
UpdateGeoMatchConstraint	Grants permission to insert or delete GeoMatchConstraint objects in a GeoMatchSet	Write	geomatchset* (p. 1875)		
UpdateIPSet	Grants permission to insert or delete IPSetDescriptor objects in an IPSet	Write	ipset* (p. 1874)		
UpdateRateBasedRule	Grants permission to modify a ratebased rule	Write	ratebasedrule* (p. 1874)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateRegexMatchSet	Grants permission to insert or delete RegexMatchTuple objects in a RegexMatchSet	Write	regexmatchset* (p. 1875)		
UpdateRegexPatternSet	Grants permission to insert or delete RegexPatternStrings in a RegexPatternSet	Write	regexpatternset* (p. 1875)		
UpdateRule	Grants permission to modify a Rule	Write	rule* (p. 1874)		
UpdateRuleGroup	Grants permission to insert or delete ActivatedRule objects in a RuleGroup	Write	rulegroup* (p. 1875)		
UpdateSizeConstraintSet	Grants permission to insert or delete SizeConstraint objects in a SizeConstraintSet	Write	sizeconstraintset* (p. 1875)		
UpdateSqlInjectionMatchSet	Grants permission to insert or delete SqlInjectionMatchTuple objects in an SqlInjectionMatchSet	Write	sqlinjectionmatchset* (p. 1875)		
UpdateWebACL	Grants permission to insert or delete ActivatedRule objects in a WebACL	Permissions management	webacl* (p. 1875)		
UpdateXssMatchSet	Grants permission to insert or delete XssMatchTuple objects in an XssMatchSet	Write	xssmatchset* (p. 1875)		

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 \(p. 1868\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1875)
rule	arn:\${Partition}:waf::\${Account}:rule/\${Id}	aws:ResourceTag/\${TagKey} (p. 1875)

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} (p. 1875)
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} (p. 1875)

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 [Available global condition 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 \(p. 1876\)](#)
- [Resource types defined by AWS WAF Regional \(p. 1882\)](#)
- [Condition keys for AWS WAF Regional \(p. 1883\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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/ * (p. 1882)		
			webacl* (p. 1883)		
CreateByteMatchSet	Grants permission to create a ByteMatchSet	Write	bytematchset* (p. 1882)		
CreateGeoMatchSet	Grants permission to create a GeoMatchSet	Write	geomatchset* (p. 1883)		
CreateIPSet	Grants permission to create an IPSet	Write	ipset* (p. 1882)		
CreateRateBasedRule	Grants permission to create a RateBasedRule	Write	ratebasedrule* (p. 1882)		
			aws:RequestTag/ \${TagKey} (p. 1883)		
			aws:TagKeys (p. 1883)		
CreateRegexMatchSet	Grants permission to create a RegexMatchSet	Write	regexmatchset* (p. 1883)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRegexPatternSet	Grants permission to create a RegexPatternSet	Write	regexpatternset* (p. 1883)		
CreateRule	Grants permission to create a Rule	Write	rule* (p. 1882)		
				aws:RequestTag/\${TagKey} (p. 1883) aws:TagKeys (p. 1883)	
CreateRuleGroup	Grants permission to create a RuleGroup	Write	rulegroup* (p. 1883)		
				aws:RequestTag/\${TagKey} (p. 1883) aws:TagKeys (p. 1883)	
CreateSizeConstraintSet	Grants permission to create a SizeConstraintSet	Write	sizeconstraintset* (p. 1882)		
CreateSqlInjectionMatchSet	Grants permission to create an SqlInjectionMatchSet	Write	sqlinjectionmatchset* (p. 1882)		
CreateWebACL	Grants permission to create a WebACL	Permissions management	webacl* (p. 1883)		
				aws:RequestTag/\${TagKey} (p. 1883)	
				aws:TagKeys (p. 1883)	
CreateWebACLMigrationCloudFront	Grants permission to create a CloudFront 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* (p. 1883)	s3:PutObject	
CreateXssMatchSet	Grants permission to create an XssMatchSet	Write	xssmatchset* (p. 1883)		
DeleteByteMatchSet	Grants permission to delete a ByteMatchSet	Write	bytematchset* (p. 1882)		
DeleteGeoMatchSet	Grants permission to delete a GeoMatchSet	Write	geomatchset* (p. 1883)		
DeleteIPSet	Grants permission to delete an IPSet	Write	ipset* (p. 1882)		
DeleteLoggingConfiguration	Grants permission to delete a LoggingConfiguration from a web ACL	Write	webacl* (p. 1883)		
DeletePermission	Grants permission to delete an IAM policy from a rule group	Permissions management	rulegroup* (p. 1883)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteRateBasedRule	Grants permission to delete a RateBasedRule	Write	ratebasedrule* (p. 1882)		
DeleteRegexMatchSet	Grants permission to delete a RegexMatchSet	Write	regexmatchset* (p. 1883)		
DeleteRegexPatternSet	Grants permission to delete a RegexPatternSet	Write	regexpatternset* (p. 1883)		
DeleteRule	Grants permission to delete a Rule	Write	rule* (p. 1882)		
DeleteRuleGroup	Grants permission to delete a RuleGroup	Write	rulegroup* (p. 1883)		
DeleteSizeConstraintSet	Grants permission to delete a SizeConstraintSet	Write	sizeconstraintset* (p. 1882)		
DeleteSqlInjectionMatchSet	Grants permission to delete an SqlInjectionMatchSet	Write	sqlinjectionmatchset* (p. 1882)		
DeleteWebACL	Grants permission to delete a WebACL	Permissions management	webacl* (p. 1883)		
DeleteXssMatchSet	Grants permission to delete an XSSMatchSet	Write	xssmatchset* (p. 1883)		
DisassociateWebACL	Grants permission to delete an association between a web ACL and a resource	Write	loadbalancer/app/* (p. 1882)		
GetByteMatchSet	Grants permission to retrieve a ByteMatchSet	Read	bytematchset* (p. 1882)		
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* (p. 1883)		
GetIPSet	Grants permission to retrieve an IPSet	Read	ipset* (p. 1882)		
GetLoggingConfiguration	Grants permission to retrieve a LoggingConfiguration	Read	webacl* (p. 1883)		
GetPermissionPolicy	Grants permission to retrieve any IAM policy attached to a RuleGroup	Read	rulegroup* (p. 1883)		
GetRateBasedRule	Grants permission to retrieve a RateBasedRule	Read	ratebasedrule* (p. 1882)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRateBasedRule	Grants permission to retrieve the array of IP addresses that are currently being blocked by a RateBasedRule	Read	ratebasedrule* (p. 1882)		
GetRegexMatchSet	Grants permission to retrieve a RegexMatchSet	Read	regexmatchset* (p. 1883)		
GetRegexPatternSet	Grants permission to retrieve a RegexPatternSet	Read	regexpatternset* (p. 1883)		
GetRule	Grants permission to retrieve a Rule	Read	rule* (p. 1882)		
GetRuleGroup	Grants permission to retrieve a RuleGroup	Read	rulegroup* (p. 1883)		
GetSampledRequests	Grants permission to retrieve detailed information for a sample set of web requests	Read	rule (p. 1882)		
			webacl (p. 1883)		
GetSizeConstraintSet	Grants permission to retrieve a SizeConstraintSet	Read	sizeconstraintset* (p. 1882)		
GetSqlInjectionMatchSet	Grants permission to retrieve an SqlInjectionMatchSet	Read	sqlinjectionmatchset* (p. 1882)		
GetWebACL	Grants permission to retrieve a WebACL	Read	webacl* (p. 1883)		
GetWebACLForResource	Grants permission to retrieve a WebACL that's associated with a specified resource	Read	loadbalancer/app/* (p. 1882)		
GetXssMatchSet	Grants permission to retrieve an XssMatchSet	Read	xssmatchset* (p. 1883)		
ListActivatedRules	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			
ListIPSets	Grants permission to retrieve an array of IPSetSummary objects	List			
ListLoggingConfigurations	Grants permission to retrieve an array of LoggingConfiguration objects	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListRateBasedRules	Grants permission to retrieve an array of RuleSummary objects	List			
ListRegexMatchSets	Grants permission to retrieve an array of RegexMatchSetSummary objects	List			
ListRegexPatternSets	Grants permission to retrieve an array of RegexPatternSetSummary objects	List			
ListResourcesForWebACL	Grants permission to retrieve an array of resources associated with a specified WebACL	List	webacl* (p. 1883)		
ListRuleGroups	Grants permission to retrieve an array of RuleGroup objects	List			
ListRules	Grants permission to retrieve an array of RuleSummary objects	List			
ListSizeConstraints	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 (p. 1882)		
			rule (p. 1882)		
			rulegroup (p. 1883)		
			webacl (p. 1883)		
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* (p. 1883)		iam:CreateServiceLinkedRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutPermissionPolicy	Grants permission to attach an IAM policy to a specified rule group, to support rule group sharing between accounts	Permissions management	rulegroup* (p. 1883)		
TagResource	Grants permission to add a Tag to a resource	Tagging	ratebasedrule (p. 1882)		
			rule (p. 1882)		
			rulegroup (p. 1883)		
			webacl (p. 1883)		
			aws:RequestTag/ \${TagKey} (p. 1883)		
			aws:TagKeys (p. 1883)		
UntagResource	Grants permission to remove a Tag from a resource	Tagging	ratebasedrule (p. 1882)		
rule (p. 1882)					
rulegroup (p. 1883)					
webacl (p. 1883)					
aws:TagKeys (p. 1883)					
UpdateByteMatch	Grants permission to insert or delete ByteMatchTuple objects in a ByteMatchSet	Write	bytematchset* (p. 1882)		
UpdateGeoMatch	Grants permission to insert or delete GeoMatchConstraint objects in a GeoMatchSet	Write	geomatchset* (p. 1883)		
UpdateIPSet	Grants permission to insert or delete IPSetDescriptor objects in an IPSet	Write	ipset* (p. 1882)		
UpdateRateBasedRule	Grants permission to insert or delete predicate objects in a rate based rule and update the RateLimit in the rule	Write	ratebasedrule* (p. 1882)		
UpdateRegexMatch	Grants permission to insert or delete RegexMatchTuple objects in a RegexMatchSet	Write	regexmatchset* (p. 1883)		
UpdateRegexPattern	Grants permission to insert or delete RegexPatternStrings in a RegexPatternSet	Write	regexpatternset* (p. 1883)		
UpdateRule	Grants permission to insert or delete predicate objects in a Rule	Write	rule* (p. 1882)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateRuleGroup	Grants permission to insert or delete ActivatedRule objects in a RuleGroup	Write	rulegroup* (p. 1883)		
UpdateSizeConstraintSet	Grants permission to insert or delete SizeConstraint objects in a SizeConstraintSet	Write	sizeconstraintset* (p. 1882)		
UpdateSqlInjectionMatchSet	Grants permission to insert or delete SqlInjectionMatchTuple objects in an SqlInjectionMatchSet	Write	sqlinjectionmatchset* (p. 1882)		
UpdateWebACL	Grants permission to insert or delete ActivatedRule objects in a WebACL	Permissions management	webacl* (p. 1883)		
UpdateXssMatchSet	Grants permission to insert or delete XssMatchTuple objects in an XssMatchSet	Write	xssmatchset* (p. 1883)		

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 \(p. 1876\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1883)
rule	arn:\${Partition}:waf-regional:\${Region}: \${Account}:rule/\${Id}	aws:ResourceTag/\${TagKey} (p. 1883)
sizeconstraintset	arn:\${Partition}:waf-regional:\${Region}: \${Account}:sizeconstraintset/\${Id}	
sqlinjectionmatchset	arn:\${Partition}:waf-regional:\${Region}: \${Account}:sqlinjectionset/\${Id}	

Resource types	ARN	Condition keys
webacl	arn:\${Partition}:waf-regional:\${Region}: \${Account}:webacl/\${Id}	aws:ResourceTag/\${TagKey} (p. 1883)
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} (p. 1883)

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 [Available global condition 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 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 \(p. 1884\)](#)

- [Resource types defined by AWS WAF V2 \(p. 1889\)](#)
- [Condition keys for AWS WAF V2 \(p. 1890\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 with a resource	Write	webacl* (p. 1889) apigateway (p. 1890) appsync (p. 1890) loadbalancer/app/ (p. 1890)		
CheckCapacity	Grants permission to calculate web ACL capacity unit (WCU) requirements for a specified scope and set of rules	Read			
CreateIPSet	Grants permission to create an IPSet	Write	ipset* (p. 1889) aws:RequestTag/\${TagKey} (p. 1890) aws:TagKeys (p. 1890)		
CreateRegexPatternSet	Grants permission to create a RegexPatternSet	Write	regexpatternset* (p. 1890) aws:RequestTag/\${TagKey} (p. 1890) aws:TagKeys (p. 1890)		
CreateRuleGroup	Grants permission to create a RuleGroup	Write	rulegroup* (p. 1889) ipset (p. 1889) regexpatternset (p. 1890)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/ \${TagKey} (p. 1890) aws:TagKeys (p. 1890)	
CreateWebACL	Grants permission to create a WebACL	Write	webacl* (p. 1889)		
			ipset (p. 1889)		
			managedruleset (p. 1889)		
			regexpatternset (p. 1890)		
			rulegroup (p. 1889)		
				aws:RequestTag/ \${TagKey} (p. 1890) aws:TagKeys (p. 1890)	
DeleteFirewallManagerManagedRulesGroups	Grants permission to delete Firewall Manager Managed Rules Groups from a WebACL if not managed by Firewall Manager anymore	Write	webacl* (p. 1889)		
DeleteIPSet	Grants permission to delete an IPSet	Write	ipset* (p. 1889)		
DeleteLoggingConfiguration	Grants permission to delete the Logging Configuration from a WebACL	Write	webacl* (p. 1889)		
DeletePermissionPolicy	Grants permission to delete the Permission Policy on a RuleGroup	Permissions management	rulegroup* (p. 1889)		
DeleteRegexPatternSet	Grants permission to delete a Regex Pattern Set	Write	regexpatternset* (p. 1890)		
DeleteRuleGroup	Grants permission to delete a Rule Group	Write	rulegroup* (p. 1889)		
DeleteWebACL	Grants permission to delete a WebACL	Write	webacl* (p. 1889)		
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* (p. 1889)		
DisassociateWebACL	Grants permission to disassociate a WebACL from an application resource	Write	apigateway (p. 1890)		
			appsync (p. 1890)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			loadbalancer/app/ (p. 1890)		
GenerateMobileSdkReleaseDownloadUrl	Grants permission to generate a download URL for the specified release of the mobile SDK	Read			
GetIPSet	Grants permission to retrieve details about an IPSet	Read	ipset* (p. 1889)		
				aws:ResourceTag/\${TagKey} (p. 1890)	
GetLoggingConfig	Grants permission to retrieve LoggingConfiguration for a WebACL	Read	webacl* (p. 1889)		
				aws:ResourceTag/\${TagKey} (p. 1890)	
GetManagedRuleSet	Grants permission to retrieve details about a ManagedRuleSet	Read	managedruleset* (p. 1889)		
GetMobileSdkReleaseInformation	Grants permission to retrieve information for the specified mobile SDK release, including release notes and tags	Read			
GetPermissionPolicy	Grants permission to retrieve a PermissionPolicy for a RuleGroup	Read	rulegroup* (p. 1889)		
GetRateBasedStats	Grants permission to retrieve the keys that are currently blocked by a rate-based rule	Read	webacl* (p. 1889)		
				aws:ResourceTag/\${TagKey} (p. 1890)	
GetRegexPatternSet	Grants permission to retrieve details about a RegexPatternSet	Read	regexpatternset* (p. 1890)		
				aws:ResourceTag/\${TagKey} (p. 1890)	
GetRuleGroup	Grants permission to retrieve details about a RuleGroup	Read	rulegroup* (p. 1889)		
				aws:ResourceTag/\${TagKey} (p. 1890)	
GetSampledRequests	Grants permission to retrieve detailed information about a sampling of web requests	Read	webacl* (p. 1889)		
GetWebACL	Grants permission to retrieve details about a WebACL	Read	webacl* (p. 1889)		
				aws:ResourceTag/\${TagKey} (p. 1890)	
GetWebACLForResource	Grants permission to retrieve the WebACL that's associated with a resource	Read	apigateway (p. 1890)		
				appsync (p. 1890)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			loadbalancer/app/ (p. 1890)		
ListAvailableManagedRuleGroups	Grants permission to retrieve an array of managed rule group versions that are available for you to use	List			
ListAvailableManagedRuleGroupsForPreview	Grants permission to retrieve an array of managed rule groups that are available for you to use	List			
ListIPSets	Grants permission to retrieve an array of IPSetSummary objects for the IP sets that you manage	List			
ListLoggingConfigurations	Grants permission to retrieve an array of your LoggingConfiguration objects	List			
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			
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* (p. 1889)		
ListRuleGroups	Grants permission to retrieve an array of RuleGroupSummary objects for the rule groups that you manage	List			
ListTagsForResource	Grants permission to list tags for a resource	Read	ipset (p. 1889)		
			regexpatternset (p. 1890)		
			rulegroup (p. 1889)		
			webacl (p. 1889)		
			aws:ResourceTag/\${TagKey} (p. 1890)		

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			
PutFirewallManageredRulesGroups [permission only]	Grants permission to create FirewallManagedRulesGroups in a WebACL	Write	webacl* (p. 1889)		
PutLoggingConfig	Grants permission to enable a LoggingConfiguration, to start logging for a web ACL	Write	webacl* (p. 1889)		iam:CreateServiceLinkedRole
PutManagedRuleSet [version]	Grants permission to enable CreateVersion or update an existing version of a ManagedRuleSet	Write	managedruleset* (p. 1889)		
			rulegroup* (p. 1889)		
PutPermissionPolicy	Grants permission to attach an IAM policy to a resource, used to share rule groups between accounts	Permissions management	rulegroup* (p. 1889)		
TagResource	Grants permission to associate tags with a AWS resource	Tagging	ipset (p. 1889)		
			regexpatternset (p. 1890)		
			rulegroup (p. 1889)		
			webacl (p. 1889)		
				aws:TagKeys (p. 1890)	
				aws:RequestTag/ \${TagKey} (p. 1890)	
				aws:ResourceTag/ \${TagKey} (p. 1890)	
UntagResource	Grants permission to disassociate tags from an AWS resource	Tagging	ipset (p. 1889)		
			regexpatternset (p. 1890)		
			rulegroup (p. 1889)		
			webacl (p. 1889)		
				aws:TagKeys (p. 1890)	
UpdateIPSet	Grants permission to update an IPSet	Write	ipset* (p. 1889)		
				aws:ResourceTag/ \${TagKey} (p. 1890)	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateManagedRuleSet	Grants permission to update The Expired date of play version in ManagedRuleSet	Write	managedruleset* (p. 1889)		
UpdateRegexPatternSet	Grants permission to update a RegexPatternSet	Write	regexpatternset* (p. 1890)	aws:ResourceTag/ \${TagKey} (p. 1890)	
UpdateRuleGroup	Grants permission to update a RuleGroup	Write	rulegroup* (p. 1889) ipset (p. 1889) regexpatternset (p. 1890)	aws:ResourceTag/ \${TagKey} (p. 1890)	
UpdateWebACL	Grants permission to update a WebACL	Write	webacl* (p. 1889) ipset (p. 1889) managedruleset (p. 1889) regexpatternset (p. 1890) rulegroup (p. 1889)	aws:ResourceTag/ \${TagKey} (p. 1890)	

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 \(p. 1884\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1890)
ipset	arn:\${Partition}:wafv2:\${Region}:\${Account}: \${Scope}/ipset/\${Name}/\${Id}	aws:ResourceTag/ \${TagKey} (p. 1890)
managedruleset	arn:\${Partition}:wafv2:\${Region}:\${Account}: \${Scope}/managedruleset/\${Name}/\${Id}	
rulegroup	arn:\${Partition}:wafv2:\${Region}:\${Account}: \${Scope}/rulegroup/\${Name}/\${Id}	aws:ResourceTag/ \${TagKey} (p. 1890)

Resource types	ARN	Condition keys
regexpatternset	arn:\${Partition}:wafv2:\${Region}:\${Account}: \${Scope}/regexpatternset/\${Name}/\${Id}	aws:ResourceTag/\${TagKey} (p. 1890)
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}	

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 [Available global condition 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 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](#) (p. 1891)
- [Resource types defined by AWS Well-Architected Tool](#) (p. 1894)
- [Condition keys for AWS Well-Architected Tool](#) (p. 1894)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateLenses	Grants permission to associate a lens to the specified workload	Write	workload* (p. 1894)		
CreateLensShare	Grants permission to an owner of a lens to share with other AWS accounts and IAM Users	Write	lens* (p. 1894)		
CreateLensVersion	Grants permission to create a new lens version	Write	lens* (p. 1894)		
CreateMilestone	Grants permission to create a new milestone for the specified workload	Write	workload* (p. 1894)		
CreateWorkload	Grants permission to create a new workload	Write		aws:RequestTag/ \${TagKey} (p. 1894) aws:TagKeys (p. 1894)	
CreateWorkloadShare	Grants permission to share a workload with another account	Write	workload* (p. 1894)		
DeleteLens	Grants permission to delete a lens	Write	lens* (p. 1894)		
DeleteLensShare	Grants permission to delete an existing lens share	Write	lens* (p. 1894)		
DeleteWorkload	Grants permission to delete an existing workload	Write	workload* (p. 1894)		
DeleteWorkloadShare	Grants permission to delete an existing workload share	Write	workload* (p. 1894)		
DisassociateLens	Grants permission to disassociate a lens from the specified workload	Write	workload* (p. 1894)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ExportLens	Grants permission to export an existing lens	Read	lens* (p. 1894)		
GetAnswer	Grants permission to retrieve the specified answer from the specified lens review	Read	workload* (p. 1894)		
GetLens	Grants permission to get an existing lens	Read	lens* (p. 1894)		
GetLensReview	Grants permission to retrieve the specified lens review of the specified workload	Read	workload* (p. 1894)		
GetLensReviewReport	Grants permission to retrieve the report for the specified lens review	Read	workload* (p. 1894)		
GetLensVersionDifference	Grants permission to get the difference between the specified lens version and latest available lens version	Read	lens* (p. 1894)		
GetMilestone	Grants permission to retrieve the specified milestone of the specified workload	Read	workload* (p. 1894)		
GetWorkload	Grants permission to retrieve the specified workload	Read	workload* (p. 1894)	aws:ResourceTag/\${TagKey} (p. 1894)	
ImportLens	Grants permission to import a new lens		Write		
ListAnswers	Grants permission to list the answers from the specified lens review	List	workload* (p. 1894)		
ListLensReviewImprovements	Grants permission to list the improvements of the specified lens review	List	workload* (p. 1894)		
ListLensReviews	Grants permission to list the lens reviews of the specified workload	List	workload* (p. 1894)		
ListLensShares	Grants permission to list all shares created for a lens	List	lens* (p. 1894)		
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* (p. 1894)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListNotifications	Grants permission to list notifications related to the account or specified resource	List			
ListShareInvitation	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	workload* (p. 1894)		
				aws:ResourceTag/ \${TagKey} (p. 1894)	
ListWorkloadShares	Grants permission to list the workload shares of the specified workload	List	workload* (p. 1894)		
ListWorkloads	Grants permission to list the workloads in this account	List			
TagResource	Grants permission to tag a Well-Architected resource	Tagging	workload* (p. 1894)		
				aws:TagKeys (p. 1894)	
				aws:RequestTag/ \${TagKey} (p. 1894)	
UntagResource	Grants permission to untag a Well-Architected resource	Tagging	workload* (p. 1894)		
				aws:TagKeys (p. 1894)	
UpdateAnswer	Grants permission to update properties of the specified answer	Write	workload* (p. 1894)		
UpdateLensReview	Grants permission to update properties of the specified lens review	Write	workload* (p. 1894)		
UpdateShareInvitation	Grants permission to update status of the specified workload share invitation	Write	workload* (p. 1894)		
UpdateWorkload	Grants permission to update properties of the specified workload	Write	workload* (p. 1894)		
UpdateWorkloadSnapshot	Grants permission to update properties of the specified workload	Write	workload* (p. 1894)		
UpgradeLensReview	Grants permission to upgrade the specified lens review to use the latest version of the associated lens	Write	workload* (p. 1894)		

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 \(p. 1891\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
workload	<code>arn:\${Partition}:wellarchitected:\${Region}:\${Account}:workload/\${ResourceId}</code>	aws:ResourceTag/\${TagKey} (p. 1894)
lens	<code>arn:\${Partition}:wellarchitected:\${Region}:\${Account}:lens/\${ResourceId}</code>	

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 [Available global condition keys](#).

Condition keys	Description	Type
<code>aws:RequestTag/\${TagKey}</code>	Filters access based on the presence of tag key-value pairs in the request	String
<code>aws:ResourceTag/\${TagKey}</code>	Filters access based on tag key-value pairs attached to the resource	String
<code>aws:TagKeys</code>	Filters access based on the presence of tag keys in the 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 \(p. 1895\)](#)

- [Resource types defined by Amazon WorkDocs \(p. 1899\)](#)
- [Condition keys for Amazon WorkDocs \(p. 1899\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 <code>InitiateDocumentVersionUpload</code> .	Write			
ActivateUser	Grants permission to activate the specified user. Only active users can access Amazon WorkDocs.	Write			
AddResourcePermissions	Grants permission to create a set of permissions for the specified folder or document.	Write			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
CreateNotification	Grants permission to configure WorkDocs to use Amazon SNS notifications.	Write			
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			
DeleteFolder	Grants permission to permanently delete the specified folder and its contents.	Write			
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			
DeleteNotificationSubscription	Grants permission to delete the specified subscription from the specified organization.	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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			
DescribeInstances [permission only]	Grants permission to describe instances.	List			
DescribeNotificationSubscriptions	Grants permission to list the specified notification subscriptions.	List			
DescribePermissions	Grants permission to view the 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
DownloadDocument [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			
GetGroup [permission only]	Grants permission to retrieve details for the specified group.	Read			
GetResources	Grants permission to get a collection of resources.	Read			
InitiateDocumentView	Grants permission to create a new document object and version object.	Write			
RegisterDirectory [permission only]	Grants permission to register a directory.	Write			
RemoveAllResources	Grants permission to remove all the permissions from the specified resource.	Write			
RemoveResourcePermissions	Grants permission to remove the permission for the specified principal from the specified resource.	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateDocument	Grants permission to update the specified attributes of the specified document.	Write			
UpdateDocumentStatus	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			

Resource types defined by Amazon WorkDocs

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

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 [Available keys for conditions](#).

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 \(p. 1900\)](#)
- [Resource types defined by Amazon WorkLink \(p. 1903\)](#)
- [Condition keys for Amazon WorkLink \(p. 1903\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateDomain	Grants permission to associate a domain with an Amazon WorkLink fleet	Write	fleet* (p. 1903)		
AssociateWebsiteAuthorizationProvider	Grants permission to associate a website authorization provider with an Amazon WorkLink fleet	Write	fleet* (p. 1903)		
AssociateWebsiteCertificateAuthority	Grants permission to associate a website certificate authority with an Amazon WorkLink fleet	Write	fleet* (p. 1903)		
CreateFleet	Grants permission to create an Amazon WorkLink fleet	Write		aws:RequestTag/\${TagKey} (p. 1903) aws:TagKeys (p. 1903)	
DeleteFleet	Grants permission to delete an Amazon WorkLink fleet	Write	fleet* (p. 1903)		
				aws:RequestTag/\${TagKey} (p. 1903) aws:TagKeys (p. 1903)	
DescribeAuditStream	Grants permission to describe the audit stream configuration for an Amazon WorkLink fleet	Read	fleet* (p. 1903)		
DescribeCompanyNetwork	Grants permission to describe the company network configuration for an Amazon WorkLink fleet	Read	fleet* (p. 1903)		
DescribeDevice	Grants permission to describe details of a device associated with an Amazon WorkLink fleet	Read	fleet* (p. 1903)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDevicePolicy	Grants permission to describe the device policy configuration for an Amazon WorkLink fleet	Read	fleet* (p. 1903)		
DescribeDomain	Grants permission to describe details about a domain associated with an Amazon WorkLink fleet	Read	fleet* (p. 1903)		
DescribeFleetMetadata	Grants permission to describe metadata of an Amazon WorkLink fleet	Read	fleet* (p. 1903)		
				aws:RequestTag/\${TagKey} (p. 1903) aws:TagKeys (p. 1903)	
DescribeIdentityProvider	Grants permission to describe the identity provider configuration for an Amazon WorkLink fleet	Read	fleet* (p. 1903)		
DescribeWebsiteCertificate	Grants permission to describe a website certificate authority associated with an Amazon WorkLink fleet	Read	fleet* (p. 1903)		
DisassociateDomain	Grants permission to disassociate a domain from an Amazon WorkLink fleet	Write	fleet* (p. 1903)		
DisassociateWebsiteAuthorizer	Grants permission to disassociate a website authorization provider from an Amazon WorkLink fleet	Write	fleet* (p. 1903)		
DisassociateWebsiteCertificate	Grants permission to disassociate a website certificate authority from an Amazon WorkLink fleet	Write	fleet* (p. 1903)		
ListDevices	Grants permission to list the devices associated with an Amazon WorkLink fleet	List	fleet* (p. 1903)		
ListDomains	Grants permission to list the associated domains for an Amazon WorkLink fleet	List	fleet* (p. 1903)		
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* (p. 1903)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListWebsiteAuthorities	Grants permission to list the website authorities for an Amazon WorkLink fleet	List	fleet* (p. 1903)		
ListWebsiteCertificates	Grants permission to list the website certificates associated with an Amazon WorkLink fleet	List	fleet* (p. 1903)		
RestoreDomainAccess	Grants permission to restore access to a domain associated with an Amazon WorkLink fleet	Write	fleet* (p. 1903)		
RevokeDomainAccess	Grants permission to revoke access to a domain associated with an Amazon WorkLink fleet	Write	fleet* (p. 1903)		
SearchEntity [permission only]	Grants permission to list devices for an Amazon WorkLink fleet	List	fleet* (p. 1903)		
SignOutUser	Grants permission to sign out a user from an Amazon WorkLink fleet	Write	fleet* (p. 1903)		
TagResource	Grants permission to add one or more tags to a resource	Tagging	fleet* (p. 1903)		
				aws:RequestTag/ \${TagKey} (p. 1903)	
				aws:TagKeys (p. 1903)	
UntagResource	Grants permission to remove one or more tags from a resource	Tagging	fleet* (p. 1903)		
				aws:TagKeys (p. 1903)	
UpdateAuditStream	Grants permission to update the audit stream configuration for an Amazon WorkLink fleet	Write	fleet* (p. 1903)		
UpdateCompanyNetwork	Grants permission to update the company network configuration for an Amazon WorkLink fleet	Write	fleet* (p. 1903)		
UpdateDevicePolicy	Grants permission to update the device policy configuration for an Amazon WorkLink fleet	Write	fleet* (p. 1903)		
UpdateDomainMetadata	Grants permission to update the metadata for a domain associated with an Amazon WorkLink fleet	Write	fleet* (p. 1903)		
UpdateFleetMetadata	Grants permission to update the metadata of an Amazon WorkLink fleet	Write	fleet* (p. 1903)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateIdentityProviderConfiguration	Grants permission to update the configuration for an Amazon WorkLink fleet	Write	fleet* (p. 1903)		

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 \(p. 1900\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
fleet	<code>arn:\${Partition}:worklink::\${Account}:fleet/\${FleetName}</code>	aws:ResourceTag/\${TagKey} (p. 1903)

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 [Available global condition 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 \(p. 1904\)](#)
- [Resource types defined by Amazon WorkMail \(p. 1914\)](#)
- [Condition keys for Amazon WorkMail \(p. 1914\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddMembersToGroup [permission only]	Grants permission to add a list of members (users or groups) to a group	Write	organization* (p. 1914)		
AssociateDelegateToMember	Grants permission to add a member (user or group) to the resource's set of delegates	Write	organization* (p. 1914)		
AssociateMemberToMember	Grants permission to add a member (user or group) to the group's set	Write	organization* (p. 1914)		
CancelMailboxExport	Grants permission to cancel an actively running mailbox export job	Write	organization* (p. 1914)		
CreateAlias	Grants permission to add an alias to the set of a given member (user or group) of WorkMail	Write	organization* (p. 1914)		
CreateGroup	Grants permission to create a group that can be used in WorkMail by calling the <code>RegisterToWorkMail</code> operation	Write	organization* (p. 1914)		
CreateInboundMailFlowRule	Grants permission to create an inbound email flow rule which	Write	organization* (p. 1914)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
[permission only]	will apply to all email sent to an organization				
CreateMailDomain [permission only]	Grants permission to create a mail domain	Write	organization* (p. 1914)		
CreateMailUser [permission only]	Grants permission to create a user in the directory	Write	organization* (p. 1914)		
CreateMobileDevice [permission only]	Grants permission to create a new mobile device access rule	Write	organization* (p. 1914)		
CreateOrganization	Grants permission to create a new Amazon WorkMail organization	Write			
CreateOutboundRule [permission only]	Grants permission to create an Outbound Rule email flow rule which will apply to all email sent from an organization	Write	organization* (p. 1914)		
CreateResource	Grants permission to create a new WorkMail resource	Write	organization* (p. 1914)		
CreateSmtpGateway [permission only]	Grants permission to register an SMTP gateway to a WorkMail organization	Write	organization* (p. 1914)		
CreateUser	Grants permission to create a user, which can be enabled afterwards by calling the RegisterToWorkMail operation	Write	organization* (p. 1914)		
DeleteAccessControlRule	Grants permission to delete an access control rule	Write	organization* (p. 1914)		
DeleteAlias	Grants permission to remove one or more specified aliases from a set of aliases for a given user	Write	organization* (p. 1914)		
DeleteEmailMonitoringConfiguration	Grants permission to delete the Email Monitoring configuration for an organization	Write	organization* (p. 1914)		
DeleteGroup	Grants permission to delete a group from WorkMail	Write	organization* (p. 1914)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteInboundMailFlowRule [permission only]	Grants permission to remove an inbound email flow rule so that it no longer applies to emails sent to an organization	Write	organization* (p. 1914)		
DeleteMailDomain [permission only]	Grants permission to remove an unused mail domain from an organization	Write	organization* (p. 1914)		
DeleteMailboxPermission [permission only]	Grants permission to delete permissions granted to a member (user or group)	Write	organization* (p. 1914)		
DeleteMobileDevice [permission only]	Grants permission to remove a mobile device from a user	Write	organization* (p. 1914)		
DeleteMobileDeviceOverride	Grants permission to delete a mobile device access override	Write	organization* (p. 1914)		
DeleteMobileDeviceRule	Grants permission to delete a mobile device access rule	Write	organization* (p. 1914)		
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* (p. 1914)		
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* (p. 1914)		
DeleteResource	Grants permission to delete the specified resource	Write	organization* (p. 1914)		
DeleteRetentionPolicy	Grants permission to delete the retention policy based on the supplied organization and policy identifiers	Write	organization* (p. 1914)		
DeleteSmtpGateway [permission only]	Grants permission to remove an SMTP gateway from an organization	Write	organization* (p. 1914)		
DeleteUser	Grants permission to delete a user from WorkMail and all subsequent systems	Write	organization* (p. 1914)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeregisterFromWorkMail	Grants permission to mark a user, group, or resource as no longer used in WorkMail	Write	organization* (p. 1914)		
DeregisterMailDomain	Grants permission to deregister a mail domain from an organization	Write	organization* (p. 1914)		
DescribeDirectories [permission only]	Grants permission to show a list of directories available for use in creating an organization	List			
DescribeEmailMonitoring	Grants permission to retrieve the configuration for an organization	Read	organization* (p. 1914)		
DescribeGroup	Grants permission to read the details for a group	List	organization* (p. 1914)		
DescribeInboundDetails	Grants permission to read the DMARC policy for a specified organization	Read	organization* (p. 1914)		
DescribeInboundMailFlowRules [permission only]	Grants permission to read the details of an inbound mail flow rule configured for an organization	Read	organization* (p. 1914)		
DescribeKmsKeys [permission only]	Grants permission to show a list of KMS Keys available for use in creating an organization	List			
DescribeMailDomains [permission only]	Grants permission to show the details of all mail domains associated with the organization	List	organization* (p. 1914)		
DescribeMailGroups [permission only]	Grants permission to show the details of all groups associated with the organization	List	organization* (p. 1914)		
DescribeMailUsers [permission only]	Grants permission to show the details of all users associated with the organization	List	organization* (p. 1914)		
DescribeMailboxExports	Grants permission to retrieve details of a mailbox export job	Read	organization* (p. 1914)		
DescribeOrganization	Grants permission to read details of an organization	List	organization* (p. 1914)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeOrganization [permission only]	Grants permission to show a summary of all organizations associated with the account	List			
DescribeOutboundMailFlowRule [permission only]	Grants permission to read the details of an outbound mail flow rule configured for an organization	Read	organization* (p. 1914)		
DescribeResource	Grants permission to read the details for a resource	List	organization* (p. 1914)		
DescribeSmtpGateway [permission only]	Grants permission to read the details of an SMTP gateway registered to an organization	Read	organization* (p. 1914)		
DescribeUser	Grants permission to read details for a user	List	organization* (p. 1914)		
DisableMailGroup [permission only]	Grants permission to disable a mail group when it is not being used, in order to allow it to be deleted	Write	organization* (p. 1914)		
DisableMailUsers [permission only]	Grants permission to disable a user mailbox when it is no longer being used, in order to allow it to be deleted	Write	organization* (p. 1914)		
DisassociateDelegate [member from the resource's set of delegates]	Grants permission to remove a member from the resource's set of delegates	Write	organization* (p. 1914)		
DisassociateMember [from a group]	Grants permission to remove a member from a group	Write	organization* (p. 1914)		
EnableMailDomain [permission only]	Grants permission to enable a mail domain in the organization	Write	organization* (p. 1914)		
EnableMailGroup [permission only]	Grants permission to enable a mail group after it has been created to allow it to receive mail	Write	organization* (p. 1914)		
EnableMailUser [permission only]	Grants permission to enable a user's mailbox after it has been created to allow it to receive mail	Write	organization* (p. 1914)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAccessControlEffects	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* (p. 1914)		
GetDefaultRetentionPolicy	Grants permission to retrieve the retention policy associated at an organizational level	Read	organization* (p. 1914)		
GetJournalingRule [permission only]	Grants permission to read the configured journaling and fallback email addresses for email journaling	Read	organization* (p. 1914)		
GetMailDomain	Grants permission to retrieve details of a given mail domain in an organization	Read	organization* (p. 1914)		
GetMailDomainDetails [permission only]	Grants permission to get the details of the mail domain	Read	organization* (p. 1914)		
GetMailGroupDetails [permission only]	Grants permission to get the details of the mail group	Read	organization* (p. 1914)		
GetMailUserDetails [permission only]	Grants permission to get the details of the user's mailbox and account	Read	organization* (p. 1914)		
GetMailboxDetails	Grants permission to read the details of the user's mailbox	Read	organization* (p. 1914)		
GetMobileDeviceEffects	Grants permission to simulate the effects of the mobile device access rules for the given attributes of a sample access event	Read	organization* (p. 1914)		
GetMobileDeviceAccessOverride	Grants permission to retrieve a mobile device access override	Read	organization* (p. 1914)		
GetMobileDeviceDetails [permission only]	Grants permission to get the details of the mobile device	Read	organization* (p. 1914)		
GetMobileDevices [permission only]	Grants permission to get a list of the mobile devices associated with the user	Read	organization* (p. 1914)		

Service Authorization Reference
Service Authorization Reference
Amazon WorkMail

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetMobilePolicyDetails [permission only]	Grants permission to get the details of the mobile device policy associated with the organization	Read	organization* (p. 1914)		
ListAccessControlRules	Grants permission to list the access control rules	Read	organization* (p. 1914)		
ListAliases	Grants permission to list the aliases associated with a given entity	List	organization* (p. 1914)		
ListGroupMembers	Grants permission to read an overview of the members of a group. Users and groups can be members of a group	List	organization* (p. 1914)		
ListGroups	Grants permission to list summaries of the organization's groups	List	organization* (p. 1914)		
ListInboundMailFlows [permission only]	Grants permission to list inbound mail flow rules configured for an organization	List	organization* (p. 1914)		
ListMailDomains	Grants permission to list the mail domains for a given organization	List	organization* (p. 1914)		
ListMailboxExports	Grants permission to list mailbox export jobs	List	organization* (p. 1914)		
ListMailboxPermissions	Grants permission to list the mailbox permissions associated with a user, group, or resource mailbox	List	organization* (p. 1914)		
ListMembersInMailGroups [permission only]	Grants permission to get a list of all the members in a mail group	Read	organization* (p. 1914)		
ListMobileDeviceAccessOverrides	Grants permission to list the mobile device access overrides	Read	organization* (p. 1914)		
ListMobileDeviceAccessRules	Grants permission to list the mobile device access rules	Read	organization* (p. 1914)		
ListOrganizations	Grants permission to list the non-deleted organizations	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListOutboundMailFlowRules [permission only]	Grants permission to list outbound mail flow rules configured for an organization	List	organization* (p. 1914)		
ListResourceDelegates	Grants permission to list the delegates associated with a resource	List	organization* (p. 1914)		
ListResources	Grants permission to list the organization's resources	List	organization* (p. 1914)		
ListSmtpGateways [permission only]	Grants permission to list SMTP gateways registered to the organization	List	organization* (p. 1914)		
ListTagsForResource	Grants permission to list the tags applied to an Amazon WorkMail organization resource	List	organization* (p. 1914)		
				aws:TagKeys (p. 1914)	
				aws:RequestTag/\${TagKey} (p. 1914)	
ListUsers	Grants permission to list the organization's users	List	organization* (p. 1914)		
PutAccessControlRule	Grants permission to add a new Access control rule	Write	organization* (p. 1914)		
PutEmailMonitor	Grants permission to add or update the email monitoring configuration for an organization	Write	organization* (p. 1914)		
PutInboundDmarcPolicy	Grants permission to enable or disable a DMARC policy for a given organization	Write	organization* (p. 1914)		
PutMailboxPermissions	Grants permission to set permissions for a user, group, or resource, replacing any existing permissions	Write	organization* (p. 1914)		
PutMobileDeviceAccessOverride	Grants permission to add or update a mobile device access override	Write	organization* (p. 1914)		
PutRetentionPolicy	Grants permission to add or update the retention policy	Write	organization* (p. 1914)		
RegisterMailDomain	Grants permission to register a new mail domain in an organization	Write	organization* (p. 1914)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterToWorkMail	Grants permission to register existing and disabled user, group, or resource for use by associating a mailbox and calendaring capabilities	Write	organization* (p. 1914)		
RemoveMembersFromGroup [permission only]	Grants permission to remove members from a mail group	Write	organization* (p. 1914)		
ResetPassword	Grants permission to allow the administrator to reset the password for a user	Write	organization* (p. 1914)		
ResetUserPassword [permission only]	Grants permission to reset the password for a user's account	Write	organization* (p. 1914)		
SearchMembers [permission only]	Grants permission to perform a prefix search to find a specific user in a mail group	Read	organization* (p. 1914)		
SetAdmin [permission only]	Grants permission to mark a user as being an administrator	Write	organization* (p. 1914)		
SetDefaultMailDomain [permission only]	Grants permission to set the default mail domain for the organization	Write	organization* (p. 1914)		
SetJournalingRules [permission only]	Grants permission to set journaling and fallback email addresses for email journaling	Write	organization* (p. 1914)		
SetMailGroupDetails [permission only]	Grants permission to set the details of the mail group which has just been created	Write	organization* (p. 1914)		
SetMailUserDetails [permission only]	Grants permission to set the details for the user account which has just been created	Write	organization* (p. 1914)		
SetMobilePolicyDetails [permission only]	Grants permission to set the details of a mobile policy associated with the organization	Write	organization* (p. 1914)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartMailboxExportJob	Grants permission to start a new mailbox export job	Write	organization* (p. 1914)		
TagResource	Grants permission to tag the specified Amazon WorkMail organization resource	Tagging	organization* (p. 1914)		
				aws:TagKeys (p. 1914) aws:RequestTag/\${TagKey} (p. 1914)	
TestInboundMailFlowRules [permission only]	Grants permission to test what rules will apply to an email with a given sender and recipient	Write	organization* (p. 1914)		
TestOutboundMailFlowRules [permission only]	Grants permission to test what rules will apply to an email with a given sender and recipient	Write	organization* (p. 1914)		
UntagResource	Grants permission to untag the specified Amazon WorkMail organization resource	Tagging	organization* (p. 1914)		
				aws:TagKeys (p. 1914) aws:RequestTag/\${TagKey} (p. 1914)	
UpdateDefaultMailboxDomain	Grants permission to update which domain is the default domain for an organization	Write	organization* (p. 1914)		
UpdateInboundMailFlowRule [permission only]	Grants permission to update the inbound email flow rule which will apply to all email sent to an organization	Write	organization* (p. 1914)		
UpdateMailboxQuota	Grants permission to update the maximum size (in MB) of the user's mailbox	Write	organization* (p. 1914)		
UpdateMobileDeviceRule	Grants permission to update a mobile device access rule	Write	organization* (p. 1914)		
UpdateOutboundMailFlowRule [permission only]	Grants permission to update the outbound email flow rule which will apply to all email sent from an organization	Write	organization* (p. 1914)		
UpdatePrimaryEmail	Grants permission to update the primary email for a user, group, or resource	Write	organization* (p. 1914)		
UpdateResource	Grants permission to update details for the resource	Write	organization* (p. 1914)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateSmtpGateway [permission only]	Grants permission to update the details of an existing SMTP gateway registered to an organization	Write	organization* (p. 1914)		
WipeMobileDevice [permission only]	Grants permission to remotely wipe the mobile device associated with a user's account	Write	organization* (p. 1914)		

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 \(p. 1904\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1914)

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 [Available global condition 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

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 \(p. 1915\)](#)
- [Resource types defined by Amazon WorkMail Message Flow \(p. 1915\)](#)
- [Condition keys for Amazon WorkMail Message Flow \(p. 1916\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

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 <code>Content</code> of email messages with the specified message ID	Read	RawMessage* (p. 1916)		
PutRawMessageContent	Grants permission to update the <code>Content</code> of email messages with the specified message ID	Write	RawMessage* (p. 1916)		

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 \(p. 1915\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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 [Available keys for conditions](#).

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 \(p. 1916\)](#)
- [Resource types defined by Amazon WorkSpaces \(p. 1921\)](#)
- [Condition keys for Amazon WorkSpaces \(p. 1922\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the Resource element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateConnectionAlias	Grants permission to associate connection aliases with directories	Write	connectionalias* (p. 1922)		
			directoryid* (p. 1922)		
AssociateIpGroup	Grants permission to associate IP access control groups with directories	Write	directoryid* (p. 1922)		
			workspaceipgroup* (p. 1922)		
AuthorizelpRules	Grants permission to add rules to IP access control groups	Write	workspaceipgroup* (p. 1922)		
CopyWorkspaceImage	Grants permission to copy a WorkSpace image	Write	workspaceimage* (p. 1922)	workspaces:DescribeWorkspaces	
				aws:RequestTag/\${TagKey} (p. 1922)	
				aws:TagKeys (p. 1922)	
CreateConnectClientAddIn	Grants permission to create an Amazon Connect client add-in within a directory	Write	directoryid* (p. 1922)		
CreateConnectionAlias	Grants permission to create connection aliases for use with cross-Region redirection	Write		aws:RequestTag/\${TagKey} (p. 1922)	
				aws:TagKeys (p. 1922)	
CreateIpGroup	Grants permission to create IP access control groups	Write		aws:RequestTag/\${TagKey} (p. 1922)	
CreateTags	Grants permission to create tags for WorkSpaces resources	Tagging		aws:RequestTag/\${TagKey} (p. 1922)	
				aws:TagKeys (p. 1922)	
CreateUpdatedWorkspaceImage	Grants permission to create an updated WorkSpace image	Write	workspaceimage* (p. 1922)		
				aws:RequestTag/\${TagKey} (p. 1922)	
				aws:TagKeys (p. 1922)	
CreateWorkspaceBundle	Grants permission to create a WorkSpace bundle	Write	workspacebundle* (p. 1922)	workspaces:CreateTags	
			workspaceimage* (p. 1922)		
				aws:RequestTag/\${TagKey} (p. 1922)	
CreateWorkspace	Grants permission to create one or more WorkSpaces	Write	directoryid* (p. 1922)		
			workspacebundle* (p. 1922)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			workspaceid* (p. 1922)		
			aws:RequestTag/ \${TagKey} (p. 1922)		aws:TagKeys (p. 1922)
DeleteClientBranding	Grants permission to delete AWS WorkSpaces Client branding data within a directory	Write	directoryid* (p. 1922)		
DeleteConnectClientAddin	Grants permission to delete an Amazon Connect client add-in that is configured within a directory	Write	directoryid* (p. 1922)		
DeleteConnectionAlias	Grants permission to delete connection aliases	Write	connectionalias* (p. 1922)		
DeleteIpGroup	Grants permission to delete IP access control groups	Write	workspaceipgroup* (p. 1922)		
DeleteTags	Grants permission to delete tags from WorkSpaces resources	Tagging		aws:RequestTag/ \${TagKey} (p. 1922)	aws:TagKeys (p. 1922)
DeleteWorkspaceBundle	Grants permission to delete WorkSpace bundles	Write	workspacebundle* (p. 1922)		
DeleteWorkspaceImage	Grants permission to delete WorkSpace images	Write	workspaceimage* (p. 1922)		
DeregisterWorkSpace	Grants permission to deregister directories from use with Amazon WorkSpaces	Write	directoryid* (p. 1922)		
DescribeAccount	Grants permission to retrieve the configuration of Bring Your Own License (BYOL) for WorkSpaces accounts	Read			
DescribeAccountMetrics	Grants permission to retrieve modifications to the configuration of Bring Your Own License (BYOL) for WorkSpaces accounts	Read			
DescribeClientBranding	Grants permission to retrieve AWS WorkSpaces Client branding data within a directory	Read	directoryid* (p. 1922)		
DescribeClientProperties	Grants permission to retrieve information about WorkSpaces clients	List	directoryid* (p. 1922)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeConnectClientAddIns	Grants permission to retrieve a list of Amazon Connect client add-ins that have been created	List	directoryid* (p. 1922)		
DescribeConnectionAliases	Grants permission to retrieve the permissions that the owners of connection aliases have granted to other AWS accounts for connection aliases	Read	connectionalias* (p. 1922)		
DescribeConnectionAliasesList	Grants permission to retrieve a list that describes the connection aliases used for cross-Region redirection	Read			
DescribeIpGroups	Grants permission to retrieve information about IP access control groups	Read	workspaceipgroup* (p. 1922)		
DescribeTags	Grants permission to describe the tags for WorkSpaces resources	Read			
DescribeWorkSpaceBundles	Grants permission to obtain information about WorkSpace bundles	List			
DescribeWorkspaces	Grants permission to retrieve information about directories that are registered with WorkSpaces	Read			
DescribeWorkspaceImagePermissions	Grants permission to retrieve information about WorkSpace image permissions	Read	workspaceimage* (p. 1922)		
DescribeWorkspaceImages	Grants permission to retrieve information about WorkSpace images	List			
DescribeWorkspaceSnapshots	Grants permission to retrieve information about WorkSpace snapshots	List	workspaceid* (p. 1922)		
DescribeWorkspaces	Grants permission to obtain information about WorkSpaces	List			
DescribeWorkspaceStatus	Grants permission to obtain the connection status of WorkSpaces	Read			
DisassociateConnectionAliases	Grants permission to disassociate connection aliases from directories	Write	connectionalias* (p. 1922)		

Service Authorization Reference
Service Authorization Reference
Amazon WorkSpaces

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateIpGroups	Grants permission to disassociate IP access control groups from directories	Write	directoryid* (p. 1922)		
			workspaceipgroup* (p. 1922)		
ImportClientBranding	Grants permission to import AWS WorkSpaces Client branding data within a directory	Write	directoryid* (p. 1922)		
ImportWorkspaceImages	Grants permission to import Bring Your Own License (BYOL) images into Amazon WorkSpaces	Write			ec2:DescribeImages ec2:ModifyImageAttribute
ListAvailableManagementRanges	Grants permission to list the available CDR ranges for enabling Bring Your Own License (BYOL) for WorkSpaces accounts	List			
MigrateWorkspaces	Grants permission to migrate WorkSpaces	Write	workspacebundle* (p. 1922)		
			workspaceid* (p. 1922)		
ModifyAccount	Grants permission to modify the configuration of Bring Your Own License (BYOL) for WorkSpaces accounts	Write			
ModifyClientProperties	Grants permission to modify the properties of WorkSpaces clients	Write	directoryid* (p. 1922)		
ModifySelfService	Grants permission to modify the self-service WorkSpace management capabilities for your users	Permissions management	directoryid* (p. 1922)		
ModifyWorkspaceDevices	Grants permission to specify which devices and operating systems users can use to access their WorkSpaces	Write	directoryid* (p. 1922)		
ModifyWorkspaceDefaultProperties	Grants permission to modify the default properties used to create WorkSpaces	Write	directoryid* (p. 1922)		
ModifyWorkspaceProperties	Grants permission to modify WorkSpace properties, including the running mode and the AutoStop period	Write	workspaceid* (p. 1922)		
ModifyWorkspaceState	Grants permission to modify the state of WorkSpaces	Write	workspaceid* (p. 1922)		
RebootWorkspace	Grants permission to reboot WorkSpaces	Write	workspaceid* (p. 1922)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RebuildWorkspace	Grants permission to rebuild WorkSpaces	Write	workspaceid* (p. 1922)		
RegisterWorkspaceDirectories	Grants permission to register directories for use with Amazon WorkSpaces	Write	directoryid* (p. 1922)		
			aws:RequestTag/\${TagKey} (p. 1922)		aws:TagKeys (p. 1922)
RestoreWorkspace	Grants permission to restore WorkSpaces	Write	workspaceid* (p. 1922)		
RevokeIpRules	Grants permission to remove rules from IP access control groups	Write	workspaceipgroup* (p. 1922)		
StartWorkspaces	Grants permission to start AutoStop WorkSpaces	Write	workspaceid* (p. 1922)		
StopWorkspaces	Grants permission to stop AutoStop WorkSpaces	Write	workspaceid* (p. 1922)		
TerminateWorkspaces	Grants permission to terminate WorkSpaces	Write	workspaceid* (p. 1922)		
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* (p. 1922)		
UpdateConnectionAliases	Grants permission to share or Unshare Connection aliases with other accounts	Permissions management	connectionalias* (p. 1922)		
UpdateRulesOfIpGroups	Grants permission to replace Rules for IP access control groups	Write	workspaceipgroup* (p. 1922)		
UpdateWorkspaceBundles	Grants permission to update the WorkSpace images used in WorkSpace bundles	Write	workspacebundle* (p. 1922)		
UpdateWorkspaceImageSharing	Grants permission to share or Unshare WorkSpace images with other accounts by specifying whether other accounts have permission to copy the image		workspaceimage* (p. 1922)		
UpdateWorkspaceImageSharing	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* (p. 1922)		

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](#) (p. 1916) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you

can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
directoryid	arn:\${Partition}:workspaces:\${Region}: \${Account}:directory/\${DirectoryId}	aws:ResourceTag/\${TagKey} (p. 1922)
workspacebundle	arn:\${Partition}:workspaces:\${Region}: \${Account}:workspacebundle/\${BundleId}	aws:ResourceTag/\${TagKey} (p. 1922)
workspaceid	arn:\${Partition}:workspaces:\${Region}: \${Account}:workspace/\${WorkspaceId}	aws:ResourceTag/\${TagKey} (p. 1922)
workspaceimage	arn:\${Partition}:workspaces:\${Region}: \${Account}:workspaceimage/\${ImageId}	aws:ResourceTag/\${TagKey} (p. 1922)
workspaceipgroup	arn:\${Partition}:workspaces:\${Region}: \${Account}:workspaceipgroup/\${GroupId}	aws:ResourceTag/\${TagKey} (p. 1922)
connectionalias	arn:\${Partition}:workspaces: \${Region}: \${Account}:connectionalias/ \${ConnectionAliasId}	aws:ResourceTag/\${TagKey} (p. 1922)

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 [Available global condition 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 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 \(p. 1923\)](#)
- [Resource types defined by Amazon WorkSpaces Application Manager \(p. 1923\)](#)
- [Condition keys for Amazon WorkSpaces Application Manager \(p. 1923\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
<code>AuthenticatePack</code> [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 [Available keys for conditions](#).

Actions, resources, and condition keys for Amazon WorkSpaces Web

Amazon WorkSpaces Web (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 Web \(p. 1924\)](#)
- [Resource types defined by Amazon WorkSpaces Web \(p. 1927\)](#)
- [Condition keys for Amazon WorkSpaces Web \(p. 1928\)](#)

Actions defined by Amazon WorkSpaces Web

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

The **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateBrowserSettings	Grants permission to associate Browser settings to web portals	Write	browserSettings* (p. 1927)		
			portal* (p. 1928)		
AssociateNetworkSettings	Grants permission to associate Network settings to web portals	Write	networkSettings* (p. 1928)		ec2:CreateNetworkInterface
					ec2:CreateNetworkInterface
AssociateTrustStores	Grants permission to associate Trust stores with web portals	Write			ec2:CreateTags
			portal* (p. 1928)		ec2:DeleteNetworkInterface
AssociateUserSettings	Grants permission to associate User settings with web portals	Write	trustStore* (p. 1928)		ec2:ModifyNetworkInterface
			portal* (p. 1928)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			userSettings* (p. 1928)		
CreateBrowserSettings	Grants permission to create browser settings	Write		aws:TagKeys (p. 1928) aws:RequestTag/kms:Decrypt \${TagKey} (p. 1928) kms:DescribeKey kms:GenerateDataKey	
CreateIdentityProvider	Grants permission to create identity providers	Write	portal* (p. 1928)		
CreateNetworkSettings	Grants permission to create network settings	Write		aws:TagKeys (p. 1928) aws:RequestTag/ \${TagKey} (p. 1928)	aws:CreateServiceLinkedRole
CreatePortal	Grants permission to create web portals	Write		aws:TagKeys (p. 1928) aws:RequestTag/kms:CreateGrant \${TagKey} (p. 1928) kms:Decrypt kms:DescribeKey kms:GenerateDataKey	aws:CreateServiceLinkedRole
CreateTrustStore	Grants permission to create trust stores	Write		aws:TagKeys (p. 1928) aws:RequestTag/ \${TagKey} (p. 1928)	
CreateUserSettings	Grants permission to create user settings	Write		aws:TagKeys (p. 1928) aws:RequestTag/ \${TagKey} (p. 1928)	
DeleteBrowserSettings	Grants permission to delete browser settings	Write	browserSettings* (p. 1927)		
DeleteIdentityProvider	Grants permission to delete identity providers	Write			
DeleteNetworkSettings	Grants permission to delete network settings	Write	networkSettings* (p. 1928)		
DeletePortal	Grants permission to delete web portals	Write	portal* (p. 1928)		
DeleteTrustStore	Grants permission to delete trust stores	Write	trustStore* (p. 1928)		
DeleteUserSettings	Grants permission to delete user settings	Write	userSettings* (p. 1928)		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateBrowserSettings	Grants permission to disassociate browser settings from web portals	Write	portal* (p. 1928)		
DisassociateNetworkSettings	Grants permission to disassociate network settings from web portals	Write	portal* (p. 1928)		
DisassociateTrustStores	Grants permission to disassociate trust stores from web portals	Write	portal* (p. 1928)		
DisassociateUserSettings	Grants permission to disassociate user settings from web portals	Write	portal* (p. 1928)		
GetBrowserSettings	Grants permission to get details on browser settings	Read	browserSettings* (p. 1927)		
GetIdentityProviders	Grants permission to get details on identity providers	Read			
GetNetworkSettings	Grants permission to get details on network settings	Read	networkSettings* (p. 1928)		
GetPortal	Grants permission to get details on web portals	Read	portal* (p. 1928)		
GetPortalServiceProviderMetadata	Grants permission to get service provider metadata information for web portals	Read	portal* (p. 1928)		
GetTrustStore	Grants permission to get details on trust stores	Read	trustStore* (p. 1928)		
GetTrustStoreCertificates	Grants permission to get certificates from trust stores	Read	trustStore* (p. 1928)		
 GetUserSettings	Grants permission to get details on user settings	Read	userSettings* (p. 1928)		
ListBrowserSettings	Grants permission to list browser settings	Read			
ListIdentityProviders	Grants permission to list identity providers	Read			
ListNetworkSettings	Grants permission to list network settings	Read			
ListPortals	Grants permission to list web portals	Read			
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			
ListUserSettings	Grants permission to list user settings	Read			
TagResource	Grants permission to add one or more tags to a resource	Tagging		aws:TagKeys (p. 1928) aws:RequestTag/\${TagKey} (p. 1928)	
UntagResource	Grants permission to remove one or more tags from a resource	Tagging		aws:TagKeys (p. 1928) aws:RequestTag/\${TagKey} (p. 1928)	
UpdateBrowserSettings	Grants permission to update browser settings	Write	browserSettings* (p. 1927)		
UpdateIdentityProvider	Grants permission to update identity provider	Write			
UpdateNetworkSettings	Grants permission to update network settings	Write	networkSettings* (p. 1928)		
UpdatePortal	Grants permission to update web portals	Write	portal* (p. 1928)		
UpdateTrustStores	Grants permission to update trust stores	Write	trustStore* (p. 1928)		
UpdateUserSettings	Grants permission to update user settings	Write	userSettings* (p. 1928)		

Resource types defined by Amazon WorkSpaces Web

The following resource types are defined by this service and can be used in the Resource element of IAM permission policy statements. Each action in the [Actions table \(p. 1924\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the 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} (p. 1928)

Resource types	ARN	Condition keys
networkSettings	arn:\${Partition}:workspaces-web:\${Region}:\${Account}:networkSettings/\${NetworkSettingsId}	aws:ResourceTag/\${TagKey} (p. 1928)
portal	arn:\${Partition}:workspaces-web:\${Region}:\${Account}:portal/\${PortalId}	aws:ResourceTag/\${TagKey} (p. 1928)
trustStore	arn:\${Partition}:workspaces-web:\${Region}:\${Account}:trustStore/\${TrustStoreId}	aws:ResourceTag/\${TagKey} (p. 1928)
userSettings	arn:\${Partition}:workspaces-web:\${Region}:\${Account}:userSettings/\${UserSettingsId}	aws:ResourceTag/\${TagKey} (p. 1928)

Condition keys for Amazon WorkSpaces Web

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

To view the global condition keys that are available to all services, see [Available global condition 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 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 \(p. 1929\)](#)
- [Resource types defined by AWS X-Ray \(p. 1932\)](#)
- [Condition keys for AWS X-Ray \(p. 1932\)](#)

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 **Resource types** column indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. 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.

For details about the columns in the following table, see [Actions table](#).

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 <code>GetTraceSummaries</code> to get a list of trace IDs	List			
CreateGroup	Grants permission to create a group resource with a name and a filter expression	Write	group* (p. 1932)		
			aws:RequestTag/ \${TagKey} (p. 1932)		
			aws:TagKeys (p. 1932)		
CreateSamplingRule	Grants permission to create a rule to control sampling behavior for instrumented applications	Write	sampling-rule* (p. 1932)		
			aws:RequestTag/ \${TagKey} (p. 1932)		
			aws:TagKeys (p. 1932)		
DeleteGroup	Grants permission to delete a group resource	Write	group* (p. 1932)		
			aws:ResourceTag/ \${TagKey} (p. 1932)		
DeleteSamplingRule	Grants permission to delete a sampling rule	Write	sampling-rule* (p. 1932)		
			aws:ResourceTag/ \${TagKey} (p. 1932)		
GetEncryptionConfig	Grants permission to retrieve the current encryption configuration for X-Ray data	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetGroup	Grants permission to retrieve group resource details	Read	group* (p. 1932)		
				aws:ResourceTag/\${TagKey} (p. 1932)	
GetGroups	Grants permission to retrieve all active group details	Read			
GetInsight	Grants permission to retrieve the details of a specific insight	Read			
GetInsightEvents	Grants permission to retrieve the events of a specific insight	Read			
GetInsightImpactGraph	Grants permission to retrieve the part of the service graph which is impacted for a specific insight	Read			
GetInsightSummary	Grants permission to retrieve the summary of all insights for a group and time range with optional filters	Read			
GetSamplingRules	Grants permission to retrieve all sampling rules	Read			
GetSamplingStatistics	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			
GetServiceGraph	Grants permission to retrieve a document that describes services that process incoming requests, and downstream services that they call as a result	Read			
GetTimeSeriesStatistics	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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTraceSummary	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			
ListTagsForResource	Grants permission to list tags for an X-Ray resource	List	group (p. 1932)		
			sampling-rule (p. 1932)		
PutEncryptionConfig	Grants permission to update the encryption configuration for X-Ray data	Permissions management			
PutTelemetryRecords	Grants permission to send AWS X-Ray daemon telemetry to the service	Write			
PutTraceSegment	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			
TagResource	Grants permission to add tags to an X-Ray resource	Tagging	group (p. 1932)		
			sampling-rule (p. 1932)		
			aws:TagKeys (p. 1932)		
			aws:RequestTag/ \${TagKey} (p. 1932)		
UntagResource	Grants permission to remove tags from an X-Ray resource	Tagging	group (p. 1932)		
			sampling-rule (p. 1932)		
			aws:TagKeys (p. 1932)		
UpdateGroup	Grants permission to update a group resource	Write	group* (p. 1932)		
			aws:ResourceTag/ \${TagKey} (p. 1932)		
UpdateSamplingRule	Grants permission to modify a sampling rule's configuration	Write	sampling-rule* (p. 1932)		
			aws:ResourceTag/ \${TagKey} (p. 1932)		

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 \(p. 1929\)](#) identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the table. For details about the columns in the following table, see [Resource types table](#).

Resource types	ARN	Condition keys
group	<code>arn:\${Partition}:xray:\${Region}:\${Account}:group/\${GroupName}/\${Id}</code>	aws:ResourceTag/\${TagKey} (p. 1932)
sampling-rule	<code>arn:\${Partition}:xray:\${Region}:\${Account}:sampling-rule/\${SamplingRuleName}</code>	aws:ResourceTag/\${TagKey} (p. 1932)

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 [Available global condition 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

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](#)